

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

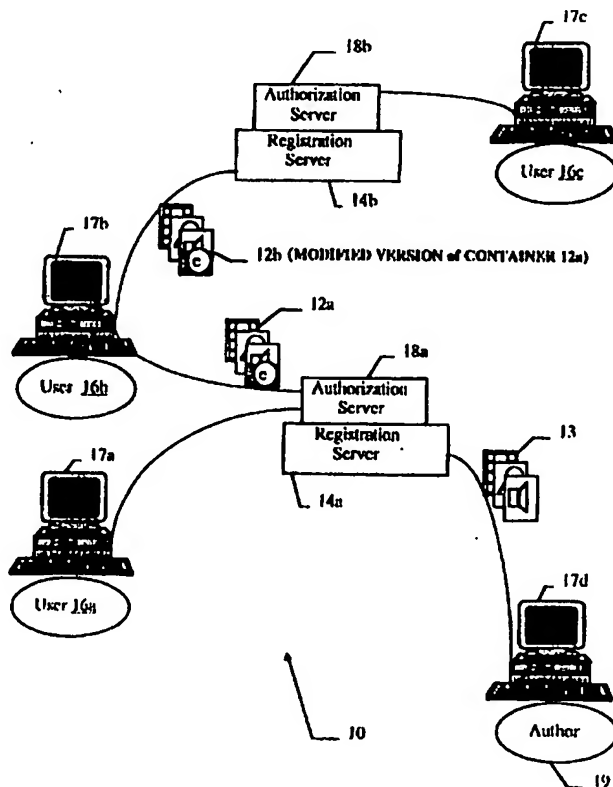
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : G06F 1/00, 17/00		A1	(11) International Publication Number: WO 97/14087
			(43) International Publication Date: 17 April 1997 (17.04.97)
(21) International Application Number: PCT/US96/16348		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date: 11 October 1996 (11.10.96)			
(30) Priority Data: 08/543,161 13 October 1995 (13.10.95) US 60/025,485 29 August 1996 (29.08.96) US			
(71)(72) Applicant and Inventor: ERICKSON, John, S. [US/US]; 27 Pierce Lane, Norwich, VT 05055 (US).			
(74) Agents: VOCK, Curtis, A. et al.; Lappin & Kusmer L.L.P., Two Hundred State Street, Boston, MA 02109 (US).		Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>	

(54) Title: SYSTEM AND METHODS FOR MANAGING DIGITAL CREATIVE WORKS

(57) Abstract

Digital Creative Works such as copyrighted electronic media are packaged in a secure electronic format, or CONTAINER, and registered on associated registration server, which serves to provide on-line licensing and copyright management for that Work. Users are connected to the registration server through a computer network or the Internet to enable data transfers and to transact licenses to utilize the media. Packaged electronic media are typically created by an author or derivative user of the work. Once the packaged media is registered on the server, the media is made available for limited use and possible license through an authorization server. This limited use is specified within the minimum permissions data set assigned to each packaged media. Without a license, users are typically permitted to view the packaged media - through a system which unpackages the media - but cannot save, print or otherwise transfer the media without obtaining auxiliary permissions to do so from the authorization server. The electronic media is authenticated through digital signatures and optional encryption.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LI	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Latvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

System and Methods for Managing Digital Creative Works

Related Applications

This application is a continuation-in-part of U.S. Patent Application No. 08/543,161, entitled "System and Methodology for Protecting Copyrighted Electronic Media," filed on October 13, 1995, and is a continuing application of Provisional Application No. 60/025,485 filed on August 30, 1996, both of which are expressly incorporated herein by reference.

Background of the Invention

The management of copyrighted material in the prior art is largely based upon hard copy technology, which attaches attribution and notification to creative works, such as copyright notices, by lines and credits. This technique is prone to significant error because notices become outdated, removed and/or ignored. Further, any copyright violation of the hard copy creative work - such as physical, unlawful copying of an article on a copying machine - is difficult to determine.

Digital media exacerbate these problems. Specifically, copyright infringement and theft has increased enormously in the computer age, particularly with respect to information data transfers through the Internet. Further, electronic email and the communication and connectivity of local and wide area networks (LANs and WANs, respectively) have facilitated unauthorized use of copyrighted materials by permitting tagging and/or enclosing of almost any electronic media, such as application software, authored text files and graphics, and musical sounds.

On-line services such as Compuserve™ and America Online™ do provide some measure of copyright protection by assessing on-line charges to the access of protected databases and to the download of selected files. However, there is little to

1 prevent that on-line user from retransmitting any downloaded files to another user
2 connected on the Internet. If the user is also connected to a network, those
3 downloaded files are also subject to remote access from yet another unauthorized
4 user.

5
6 The problems associated within electronic copyright infringement are well
7 known, particularly by those parties injured by the unauthorized use of copyrighted
8 materials. For example, the unauthorized copying of copyrighted magnetic diskettes,
9 and the electronic email and tagging and/or enclosing of copyrighted files can
10 result in a direct monetary loss to the owner of the copyrighted works, in addition
11 to an unaccounted for gain for the unauthorized user. With the expansion of the
12 Internet and other computerized networks, the aggregate amount of such losses and
13 gains is substantial.

14
15 Even the U.S. Commerce Department recognizes that serious copyright
16 problems exist with the burgeoning growth of electronic data transfers between
17 networked computers and particularly through the Internet. Early in September
18 1995, for example, the Commerce Department issued a white paper entitled
19 "Intellectual Property and the National Information Infrastructure." The paper
20 highlights the need to protect copyrighted information that is resident in cyberspace,
21 where unauthorized users can copy original works of authorship, including movies
22 and books, by pressing a couple of keystrokes. See, V. Sussman, Copyright wrong? A
23 fight brews over who gets to own the future (cyberspace), U.S. News & World
24 Report, September 18, 1995, v119 n11 p99(1).

25
26 In the prior art, methods have been developed to enhance copyright
27 protection of electronic media. For example, AT&T Bell Laboratories has developed
28 a system which makes tiny adjustments to the spacing between words so that every
29 copy of a document utilizing the system is "unique." These electronic adjustments
30 are detectable by computers only because they are too small for the human eye to

1 notice. By way of another example, Digimarc, a company in Portland, Oregon,
2 recently announced a system that encodes data into an image by carefully adjusting
3 the digital representation of individual pixels. As in the AT&T system, the encoded
4 data is not noticeable to the eye and enables some traceability of unauthorized
5 copyright uses. See, S. Steinberg, editor of Wired Magazine, Los Angeles Times
6 column, p2, part D, August 31 (1995).

7
8 However, such systems operate only to detect unauthorized usage of
9 copyrighted works in digital form. They do not manage the access to copyrighted
10 works, nor do they provide any systematic way of controlling the rights to
11 copyrighted electronic media.

12
13 More particularly, the tracing of copyright clearances to users of copyrighted
14 electronic media in the prior art is a tedious and often impossible task. Specifically,
15 authors and multimedia developers have had only two practical methods for
16 protecting their copyrights of electronic works: one method is to rely upon copyright
17 laws and international treaties to prohibit unauthorized use of the media; and the
18 other is to encrypt the data, so that access is restricted to those users with a
19 decryption key.

20
21 In the first method, media developers typically do nothing; or they attach a
22 textual copyright warning - sometimes called a "watermark" - to the media. This
23 type of "protection" ensures free access to the media, but it works only for those
24 honest users and derivative developers who view the work and decide whether they
25 want to license it. However, users and developers of such media cannot be sure of
26 the authorship or integrity of the media. Authenticity is thus sometimes increased by
27 restricting access to the media, such as through the use of a password. By way of
28 example, a password-protected World Wide Web page provides some measure of
29 authenticity, but also discourages the open and free propagation of the information
30 in the media.

1
2 In the second method, media developers can utilize powerful encryption
3 tools, readily available in the public domain, such as those tools based on the RSA
4 public key algorithm (Rivest, Shamir, & Adleman, 1977). However, the use of
5 encryption to protect copyrights only serves to restrict access to the information
6 within the media, like the password described above. Moreover, after the work is
7 decrypted on the recipient's computer, the problems of copyright heritage and
8 permissions for derivative development and use of the media remain.

9
10 These two methods favor either the user or the owner of the media. In the first
11 method, for example, there is no electronic protection coupled to the media; and it
12 thus favors the free and fair use of the media at the expense of the owners' rights. On
13 the other hand, the second method of encryption favors the owners' rights, at least to
14 a degree. Neither method affords both fair use and ownership protection; and
15 neither provides for automatic management of media rights, including the
16 controlled access to media in derivative works. Further, these methods do not
17 intervene in managing copyrights, and are beneficial only after the copyright issue
18 becomes a problem.

19 20 Objects of the Invention

21
22 It is one object of the invention to provide systems and methodologies to
23 protect the rights of intellectual property owners while promoting open and free
24 sharing of information.

25
26 Another object of the invention is to provide methods for ensuring that
27 benefits owed to owners, publishers and creators of creative works accrue to such
28 entities.

1 Still another object of the invention is to provide methods and systems for
2 crediting authors, publishers and creators of electronic multimedia objects that
3 include digital creative works.

4
5 Other objects of the invention provide tools to acquire, publish, distribute,
6 and disseminate multimedia objects to strengthen ownership and attribution of the
7 underlying digital creative work.

8
9 Another object of the invention provides systems and methods for packaging
10 and unpackaging digital creative works within a data container to facilitate the
11 management of that work.

12
13 Another object of the invention provides systems and methods for attaching
14 copyright notices and other attributes to digital creative works.

15
16 Other objects of the invention provide for (a) locating source works of
17 derivative authors of digital creative works, (b) obtaining releases and permissions
18 to incorporate another work or part of another work into the digital creative work,
19 (c) determining the source and attributes of digitally creative works, (d) promotion
20 of communication directly to the author or owner of the digital works, (e) security
21 and authentication of transactions and the digital work, and (f) the automation of
22 rights management, such as acquisition, administration, and authorization of digital
23 creative works.

24
25 It is still another object of the invention to provide systems and
26 methodologies to manage copyrighted electronic media, thereby solving or reducing
27 the problems of the prior art.

28

1 Yet another object of the invention is to provide a method for maintaining an
2 electronic bibliographic record of successive data transfers of protected electronic
3 media.

4
5 Still another object of the invention provides systems and methods for
6 packaging and unpackaging electronic media within an electronic container to
7 facilitate the management of copyrighted electronic media.

8
9 These and other objects of the invention will be apparent from the description
10 which follows.

11
12 Summary of the Invention

13
14 As used herein, a "copyrighted work" means any work that is authored and
15 protected by U.S. and international copyright laws, including, without limitation,
16 literary works; musical works, including any accompanying words; dramatic works,
17 including any accompanying music; pantomimes and choreographic works;
18 pictorial, graphic, and sculptural works; motion pictures and other audiovisual
19 works; sound recordings; and architectural works. "Electronic media" means any
20 electronic form or digital representation of a copyrighted work.

21
22 As used herein, a "Digital Creative Work" means any electronic media,
23 multimedia content element, electronic creative work, and in particular work such as
24 authored and protected by U.S. and international copyright laws, including, without
25 limitation, any of the following in digital or electronic form: literary works; musical
26 works, including any accompanying words; dramatic works, including any
27 accompanying music; pantomimes and choreographic works; pictorial, graphic, and
28 sculptural works; motion pictures and other audiovisual works; sound recordings;
29 and architectural works. Further, a Digital Creative Work can include multimedia
30 content elements that have two or more creative works, such as a digital image and

1 associated digital audio. As such, a Digital Creative Work includes any electronic
2 form or digital representation of a copyrighted work, including multimedia objects,
3 and including any form or digital representation (1) stored within computer memory
4 or other electronic memory, (2) resident on CD-ROM and/or magnetic disk or tape,
5 (3) transmitted as a digital file through email, an on-line service such as
6 Compuserve™, the World Wide Web (WWW), Intranet and/or the Internet; and (4)
7 communicated as a digital file within or into a computer network, such as a LAN or
8 WAN, and including any communication obtained through remote access. Further, a
9 Digital Creative Work can include, but is not limited to, digital embodiments of a
10 creative expression, such as digital audio (eg: WAV, SND, AIFF, AU), digital music
11 sequences (eg: MIDI), digital video (eg: AVI, MOV, MPEG), digital images and
12 graphics (eg: GIF, BMP, TIFF, JPEG, FlashPix), word processing files (eg: DOC), and
13 spreadsheet files (eg: XLS).

14

15 As used herein, "CONTAINER" means an electronic or digital entity that is
16 constructed according to the invention to enable the use of, control of, access to,
17 and/or licensing of the Digital Creative Work. The CONTAINER is a logical entity
18 that is preferably based on object technology such as C, C++, Visual Basic,
19 Microsoft's ActiveX™ Controls, Microsoft's OLE™ Controls, Apple's OpenDoc™,
20 and Sun Microsystem's Java™ applet component technologies. Accordingly, a
21 CONTAINER of the invention is a data container that includes a data portion with
22 the Digital Creative Work, and an executable portion that typically adds
23 functionality to Web Sites, desktop applications and development tools in order to
24 manage that Digital Creative Work. A CONTAINER can be distributed through
25 many channels, such as through the Internet, CD ROM, or magnetic media.
26 Further, a CONTAINER can be formed of different parts that are located remotely to
27 one another; though the different parts are linked to maintain attribution within the
28 CONTAINER.

29

1 As used herein, "METADATA" refers to data associated or encapsulated with
2 a CONTAINER and includes a plurality of data pertinent to copyright management,
3 including, for example, ownership identification and contact information, rights
4 administration identification and contact information, creatorship identification and
5 contact information, an identification and address of a registration server, listings of
6 antecedent and related objects, and licensing terms and conditions.

7
8 As used herein, a "DIGITAL CONTRACT" means a contract secured through
9 licensing activity between a registration server and a user of a Digital Creative Work.
10 The Digital Contract includes a textual expression of enhanced permissions for use
11 of the Digital Creative Work and may or may not be accompanied by an upgrade of
12 the operational controls such as the ability to print, save and/or edit the Digital
13 Creative Work.

14
15 As used herein, "SYSTEM EXTENSION" means an operating system
16 extension or "plug-in" that each user obtains prior to use and/or manipulation of
17 one or more CONTAINERS. Specifically, the SYSTEM EXTENSION operates in
18 conjunction with the operating system of a computer to recognize CONTAINERS
19 and to permit authorized operations on the CONTAINER's METADATA and/or
20 Digital Creative Works. When needed, the EXTENSION can and will be
21 downloaded from various trusted locations and such as described herein so as to
22 render Digital Creative Works within CONTAINERS. However, the EXTENSION is
23 generally resident on a user's computer so as to obviate the need to continually
24 download the EXTENSION and to improve network efficiency.

25
26 As used herein, "OBJECT" means an instantiation such as an icon, graphic or
27 other visual, on a computer, which is, or which refers to, or which points to an object
28 such as a CONTAINER. Typically, an OBJECT is viewable within an application
29 such as a Web browser such that a user directly views authorized content of the
30 Digital Creative Work. However, for example, a user can select or "click" the

1 OBJECT with a computer mouse to gain additional information in and to the
2 CONTAINER and/or to obtain additional licenses to the OBJECT's Digital Creative
3 Works. The OBJECT thus instantiates the existence of the Digital Creative Work in a
4 composition such as a CONTAINER. In the usual case, for example, a Digital
5 Creative Work within a CONTAINER is actually an image (i.e., the "OBJECT") on a
6 user's computer. In the preferred embodiment of the invention, the user will view an
7 OBJECT and not notice anything different about the Digital Creative Work until the
8 user tries to operate on the OBJECT in ways that are prohibited. For example, when
9 a user attempts to click on the OBJECT, or to print the OBJECT, or to copy the
10 OBJECT to another file, or to attempt other operations that are restricted, the
11 EXTENSION takes over and informs the user that such operations are prohibited
12 without an additional license to the Digital Creative Work. An OBJECT can be
13 formed of a group of OBJECTS. Once permissions or licenses are granted to perform
14 additional operations, such as copying, the DIGITAL CREATIVE WORK and
15 METADATA remain linked during the copying process so that the user copies the
16 CONTAINER, preserving attribution and facilitating the further management of the
17 Digital Creative Work. It is important to note that an OBJECT instantiates a
18 CONTAINER which itself can exist locally, e.g., within internal memory, and/or
19 remotely across one or more sites on the Internet. The invention communicates an
20 OBJECT to a user through a file or a continuous data stream: in the first case, the
21 OBJECT is rendered to the user after the complete data set is received; and in the
22 second case the OBJECT is rendered as the data is received through the
23 communication link.

24

25 As used herein, "TOOL BOX" or "TOOLBOX" means a software application
26 that is used to create or augment a CONTAINER. Typically, the TOOL BOX is
27 resident on a computer to facilitate the management of Digital Creative Works from
28 the author or creator's desktop computer.

29

1 As used herein, "PACKAGER" means an application which creates or
2 augments a CONTAINER. Typically, the PACKAGER operates in a batch mode and
3 is used in high-volume generation of CONTAINERS for creators and owners of large
4 amounts of digital creative works. By way of another example, the PACKAGER can
5 package HTML documents, i.e., Web pages, so that a user of the Web page is
6 actually within an OBJECT that is likely composed of other OBJECTs.

7
8 As used herein, a "VIEWER" refers to software and/or hardware which
9 renders the Digital Creative Work of a CONTAINER to a user. For example, a
10 CONTAINER can be associated with a web page that is accessed by users of the
11 Internet. In order to perceive the CONTAINER, and in particular the Digital
12 Creative Work associated with the CONTAINER, the user's host computer calls on
13 the appropriate media "viewer" service registered with the computer's operating
14 system. If the Digital Creative Work is, for example, a GIF file, the computer tells the
15 SYSTEM EXTENSION to do the rendering and the SYSTEM EXTENSION, in turn,
16 calls on a GIF viewer or renderer to display the GIF (i.e., the Digital Creative Work
17 in this example) to the user. Similarly, a VIEWER can refer to rendering software of
18 JPEGs, AVIs, PDFs, MIDs, etc. Indirectly, the VIEWER is sometimes embodied with
19 the SYSTEM EXTENSION or as separate software specific to the invention so as to
20 render, for example, a Digital Contract. More particularly, when asked by the user
21 (e.g., with the "click" of a computer mouse), the EXTENSION renders the associated
22 Digital Creative Works with a VIEWER specifically designed to view the Digital
23 Contract. The VIEWER also refers to a computer subsystem, operable by a user
24 desiring to manipulate one or more CONTAINERS that contain either (a) a shell
25 extension which responds to direct manipulation, at the computer, of OBJECTS
26 referring to CONTAINERS, or (b) an object control, which is used to display
27 CONTAINERS - or portions of CONTAINERS - within other applications. By way of
28 example, an object control of the invention can include ActiveX Control that permits
29 display of an OBJECT, within an application such as a web browser, that links the
30 computer to the CONTAINER.

1
2 As used herein, "REGISTRY" generally refers to a registration server that
3 registers CONTAINERS and which operates to manage Digital Creative Works. A
4 user of a particular CONTAINER communicates to the REGISTRY via on-line
5 communication to obtain auxiliary permissions to the Digital Creative Work therein.
6 The CONTAINER contains information in the METADATA which specifies the
7 "home" or licensing site assigned to the CONTAINER. By way of example, when a
8 user clicks on an OBJECT to request auxiliary use of the Digital Creative Work, the
9 CONTAINER automatically prompts the EXTENSION to locate and connect with
10 the assigned REGISTRY through Internet communication. In certain aspects of the
11 invention, the REGISTRY includes a separate registration server and an
12 authorization server. The registration server is used to register CONTAINERS, and
13 the authorization server is used to authorize auxiliary uses of CONTAINERS, such
14 as to provide licensing to the Digital Creative Works therein. However, the
15 REGISTRY is typically a single registration server that operates as a registration
16 server and as an authorization server to negotiate licenses with on-line users of
17 Digital Creative Works.

18
19 In one aspect, the invention applies object technology to the Digital Creative
20 Work to form a data CONTAINER including the data content of the Digital Creative
21 Work and other attributes contained in METADATA. These attributes can include
22 operations, services and information that describe or operate on the METADATA
23 and/or Digital Creative Work as appropriate to the user according to the minimum
24 and/or auxiliary permissions granted within the METADATA. In another aspect,
25 the attributes and content of a CONTAINER are distributed between (a) the local
26 system, i.e., where a user views and/or manipulates the CONTAINER, and (b) a
27 registration server to which it refers across the Internet. The registration server
28 further can contain attributes that, for various reasons such as volatility, security, or
29 efficiency, cannot or should not travel to the local system.

1
2 In another aspect, a repository system provides file images, i.e., persistence
3 data, of CONTAINERS as well as resources and data referred to by CONTAINERS
4 but not held in attributes at the registration server.

5
6 In one aspect of the invention, a user at a computer accesses a particular
7 CONTAINER through a set of property pages (e.g., tabbed dialog boxes), or
8 "templates," that are available through the CONTAINER wherever it appears. For
9 example, where an OBJECT for a CONTAINER appears in a screen rendering of a
10 Web browser, a mouse click onto the OBJECT brings up its associated property
11 pages to show information and to provide access to features such as email and
12 authentication to the associated digital creative work.

13
14 In still another aspect, and as described herein, creators or authors of digital
15 creative works bind content and attributes into a CONTAINER; and register new
16 CONTAINERS through a locally resident TOOL BOX which facilitates the flexible
17 design of the CONTAINER's property pages and feature selections. In still another
18 aspect, the TOOL BOX also automates the organization and maintenance of the
19 heritage of the Digital Creative Work, such as when the CONTAINER includes
20 works from various authors.

21
22 In another aspect, one or more CONTAINERS can be, and preferably are,
23 registered at the REGISTRY, which preferably is a secured registration server system
24 remote from the viewing capabilities of the SYSTEM EXTENSION or VIEWER. In
25 this aspect, the REGISTRY (a) retains information to validate the credentials and/or
26 authenticity of a TOOL BOX, attempting to register a work, or a CONTAINER; and
27 (b) supplies remote services and data. The REGISTRY can also supply attribute data
28 obtained indirectly from a content provider's existing legacy database.

29

1 In accord with preferred aspects of the invention, access to OBJECTS is
2 generally "open" such that any user can view the associated Digital Creative Work.
3 The SYSTEM EXTENSION in this aspect is thus ubiquitous, as are most or all
4 supplementary VIEWERS. That is, when a VIEWER is called by the EXTENSION,
5 the invention preferably utilizes handshaking standard such as Microsoft's code
6 signing standard. Such a standard uses digital signature technology that helps one
7 application make sure that it is talking to the authentic version of another
8 application. Accordingly, the SYSTEM EXTENSION in this aspect is sure to call the
9 correct VIEWER and not some other viewer that does damage to the DIGITAL
10 WORK or CONTAINER.

11
12 In one aspect, the invention provides a method of packaging a digital creative
13 work, including the steps of: encapsulating the work within a data container;
14 encapsulating metadata within the container; and integrating, with the container,
15 means for accessing the work and the metadata. In another aspect, the step of
16 integrating further comprises the step of integrating, with the container, means for
17 rendering the work. The method can also include any of the following steps:
18 integrating, with the container, means for printing the work; integrating, with the
19 container, means for copying the work; integrating, with the container, means for
20 viewing the work; integrating, with the container, means for controlling use of the
21 work; integrating, with the container, means for limiting use of the work;
22 integrating, with the container, means for disallowing use of the work; integrating,
23 with the container, means for operating on the metadata; integrating, with the
24 container, means for providing email to one or more external addresses; integrating,
25 with the container, means for providing web access to one or more WWW addresses;
26 integrating, with the container, means for providing interactive licensing to the
27 work; integrating, with the container, means for providing a link to a digital contract
28 for the work; integrating, with the container, means for updating the metadata; and
29 integrating, with the container, means for displaying descriptive information.

1
2 The descriptive information can include one or more of the following:
3 authorship information, historical information, ownership information, date
4 information, time information, and bibliographic information. It can further include
5 a digital signature to verify authenticity of the work.
6

7 The method of the invention can also include the step of forming the data
8 container as a plurality of associated data that are distributed across one or more of
9 the following: a computer network, the Internet, a LAN, a WAN, an on-line service,
10 and an Intranet. Further, the work can be selected from the group of digital images
11 and graphics, digital photos, digital audio, digital video, digital music sequences,
12 word processing files, spreadsheet files, and mixtures thereof. For example, the
13 digital images and graphics can include JPEG, GIF, BMP, TIFF and mixtures thereof.
14 Similarly, the digital audio can include WAV, SND, AIFF, AU and mixtures thereof.
15 Further, the digital music sequence can include MIDI; and the digital video can
16 include AVI, MOV, MPEG and mixtures thereof. The word processing programs can
17 include, among others, Microsoft Word™, Novell WordPerfect™ and mixtures
18 thereof. Likewise, the spreadsheet programs can include, among others, Microsoft
19 Excel™.
20

21 The step of encapsulating metadata can include the step of encapsulating
22 copyright management information. The copyright management information can
23 include any of ownership identification information, ownership contact information,
24 rights administration information, rights administration contact information,
25 creatorship information, authorship information, creator contact information, author
26 contact information, listings of antecedent object information, listings of related
27 object information, licensing terms, licensing conditions, publisher information, and
28 ownership credits. These can further include email addresses, web access addresses,
29 and mixtures thereof. The step of encapsulating metadata can further include the

1 step of encapsulating registration data, the registration data identifying an
2 associated registration server capable of administrating the data container.

3
4 Preferably, the metadata is modifiable and accessible through on-line
5 communication with the registration server. Accordingly, the method can include
6 the step of storing at least part of the metadata at a database of the registration
7 server, or the step of down-loading at least part of the metadata from the registration
8 server.

9
10 The methods of the invention can also include the step of providing a user
11 interface to the data container to review at least part of the metadata on a computer.
12 The user interface is preferably displayable on the computer and is selectable by a
13 user of the computer to modify information therein.

14
15 In another aspect, the step of encapsulating metadata further includes the step
16 of encapsulating, with the data container, minimum permissions data, the minimum
17 permissions data specifying one or more operations that can be performed on the
18 work without a license to the work.

19
20 In still another aspect, the step of encapsulating metadata further includes the
21 step of encapsulating, with the data container, minimum permissions data, the
22 minimum permissions data specifying a default contract to the work, the default
23 contract specifying a minimum set of operations that can be performed by
24 applications on the work. Such operations, for example, include drag and drop
25 operations, printing operations, editing operations, activating operations, saving
26 operations, and viewing operations.

27
28 The step of integrating means for accessing the work and the metadata can
29 include the step of integrating, with the container, one or more of the following:
30 means for encoding the metadata, means for compressing the metadata, means for

1 manipulating the metadata, means for encrypting the metadata, means for decoding
2 the metadata, and means for decrypting the metadata. Similarly, the step of
3 integrating means for accessing the work and the metadata can include the step of
4 integrating, with the container, one or more of the following: means for encoding the
5 work, means for compressing the work, means for manipulating the work, means for
6 encrypting the work, means for decoding the work, and means for decrypting the
7 work.

8
9 In another aspect, the step of encapsulating the work further includes the step
10 of encrypting the work. Alternatively, the step of encapsulating metadata can
11 include: the step of associating a metadata template with the container, the metadata
12 template describing registration with a registration server; or the step of associating
13 a metadata template with the container, the metadata template specifying properties
14 of the container used to register the container with a registration server. A further
15 step can include specifying, within the template, a display interface used to view the
16 properties.

17
18 In another method of the invention, the step of encapsulating metadata
19 includes the step of associating a metadata template with the container, the metadata
20 template identifying user-selectable optional properties of the container. Further, the
21 step of encapsulating metadata can include the step of associating a metadata
22 template with the container, the metadata template specifying requirements and
23 rules associated with the work.

24
25 Certain aspects of the invention include providing, with the metadata
26 template, a user interface suitable for viewing information related to the metadata
27 and the work; and/or providing different metadata templates corresponding to
28 different types of works; and/or providing different metadata templates
29 corresponding to different licensing models.

1

2 One method of the invention includes, with the step of encapsulating
3 metadata, the step of associating, with the container, operations that can be
4 performed on the work.

5

6 In still another aspect, each registration server provides on-line
7 administration of the container and has user-selectable registration templates for
8 associating metadata with the container, at least part of the metadata being
9 modifiable over a lifetime of the container.

10

11 Further, the step of encapsulating metadata can include the step of
12 associating, with the container, requirements of specific parties having rights in or to
13 the work. The requirements can include a requirement to obtain a license to the
14 work prior to additional use of the work. The requirements can also include a
15 requirement of obtaining information about entities desiring access to the work.
16 Such information can include address and billing information of the entities. The
17 entities can include one or more of an individual, a partnership, a company, a
18 government agency, and an educational institution.

19

20 In another aspect, the step of encapsulating metadata can include the step of
21 encapsulating information indicative of one or both of an owner and creator of the
22 media, and further include the step of communicating with one or both of the owner
23 and creator through one or both of email and web page access. The steps of
24 encapsulating can be made through object-based technology. Typically, the
25 container is formed with object-based technology such as of OLE™, ActiveX™,
26 OpenDoc™, and hybrid OLE™/OpenDoc™.

27

28 The invention also provides a method of accessing a digital creative work,
29 including: installing a system extension onto a computer, the extension including (i)
30 means for operating in conjunction with an operating system controlling the

1 computer; (ii) means for accessing a data container having the work and metadata,
2 including minimum permissions data, attached thereto, the minimum permissions
3 data specifying one or more operations that can be performed on the work without a
4 license to the work; and (iii) means for recognizing the minimum permissions data
5 and for enabling a user of the computer to use the work in accord with the specified
6 operations; and accessing the container and using the work in accord with the
7 specified operations.

8
9 The step of installing a system extension can include the step of distributing
10 the extension to the computer with a computer operating system; and/or the step of
11 distributing the extension to the computer from one or more content provider sites,
12 the content provider sites creating the media; and/or distributing the extension to
13 the computer with creativity tools; and/or utilizing image and graphic creativity
14 tools selected from the group of Adobe Photoshop™, Fractal Design Painter™,
15 CorelDraw; and/or utilizing multimedia authoring tools selected from the group of
16 Macromedia Director™, Macromedia Authorware™, Asymetrix Toolbook™,
17 Aimtech IconAuthor™; and/or utilizing web authoring tools selected from the
18 group of Microsoft FrontPage™, Adobe PageMill™, Adode SiteMill™, SoftQuad
19 HoTMetaL Pro™, Corel Web.Designer™; and/or utilizing sound editing tools
20 selected from the group of Macromedia SoundEdit Pro™ and DigiDesign Pro
21 Tools™; and/or utilizing video editing tools selected from the group of Avid Media
22 Suite™, Asymetrix Digital Video Producer™, Adobe Premiere™; and/or
23 distributing the extension to the computer with web browsers selected from the
24 group of Netscape Navigator™ and Microsoft Internet Explorer™.

25
26 By way of example, the creativity tools of the invention can include one or
27 more of the following: Microsoft Word™, Microsoft Excel™, Microsoft
28 Powerpoint™, and Novell WordPerfect™.

29

1 In another aspect, the container is stored in a remote database, and the
2 methods of the invention include the step of accessing at least part of the container
3 through on-line communication with the database. For example, the step of
4 accessing part of the container through on-line communication can include one or
5 more of the following: communication through the Internet, communication through
6 a computer network, and communication through the Intranet; and/or utilizing a
7 file data stream wherein rendering of the work is possible only after all data
8 representative of the work is present at the computer; and/or utilizing a continuous
9 data stream wherein rendering of the work is possible, in part, with concurrent
10 arrival, at the computer, of data representative of the work.

11
12 In one aspect, the container is stored on a CD-ROM, and the method includes
13 the step of accessing that part of the container through communication with a CD-
14 ROM drive. Alternatively, for example, the container is stored on a magnetic data
15 disk, and the invention includes the step of accessing part of the container through
16 communication with a disk drive. In still another example, the container is stored
17 within internal memory of the computer, and the method includes the step of
18 accessing part of the container within internal memory.

19
20 In still another aspect, the system extension includes means for recognizing
21 registration data within the metadata, the registration data identifying an associated
22 registration server capable of administering the data, and the method includes the
23 step of contacting the registration server to negotiate, on-line, a license to the work.
24 An additional step can include contacting the registration server to negotiate for
25 auxiliary permissions data, the auxiliary permissions data specifying auxiliary uses
26 of the media that is licensed beyond the authorized use specified in the minimum
27 permissions data.

28
29 In another aspect, the extension can include: means for recognizing the
30 auxiliary permissions data and for enabling the user to use the work in accord with

1 the auxiliary uses; and/or means for recognizing registration data within the
2 container, the registration data identifying an associated registration server capable
3 of administrating the data, and can further include the step of contacting the
4 registration server to authenticate the work; and/or means for prohibiting
5 unauthorized uses of the work when the unauthorized uses exceed the operations
6 specified in the minimum permissions data. Such unauthorized uses of the media
7 can include, for example, drag-and-drop operations on the computer, copying,
8 saving and/or printing the work.

9
10 Typically, the auxiliary permissions specify a set of operations that can be
11 performed on the work after executing a digital contract to the work. The auxiliary
12 permissions are usually obtained through one of email or web access.

13
14 The invention also provides improvements to an operating system of the type
15 which facilitates control and communication of a digital data processor. A plug-in
16 extension is used to manipulate copyrighted electronic media, the extension having
17 means for opening a data container having a digital creative work and minimum
18 permissions data attached thereto. The minimum permissions data specifies one or
19 more operations that can be performed on the work without a license to the work.
20 The extension recognizes the minimum permissions data and enables a user of the
21 processor to use the work in accord with the specified operations.

22
23 The container can also have metadata attached thereto. The metadata
24 typically has one or more of ownership identification information, ownership
25 contact information, rights administration information, rights administration contact
26 information, creatorship information, authorship information, creator contact
27 information, author contact information, listings of antecedent object information,
28 listings of related object information, licensing terms, licensing conditions, publisher
29 information, and ownership credits, and wherein the extension comprises means for
30 reviewing the metadata selectively.

1
2 In another aspect, the invention provides a plug-in operating system
3 extension, including: means for operating in conjunction with an operating system
4 controlling a digital data processor; means for recognizing a data container having
5 digital creative works and minimum permissions data attached thereto, minimum
6 permissions data specifying one or more operations that can be performed on the
7 work without a license to the work; and means for opening the container and
8 enabling a user of the processor to use the work in accord with the specified
9 operations.

10
11 In this aspect, the container can have registration information attached
12 thereto, the registration information specifying a registration server capable of
13 administering the container, and can further include means for recognizing the
14 registration information and for communicating with the registration server to
15 acquire properties associated with the container.

16
17 The container can have registration information attached thereto, the
18 registration information specifying a registration server capable of administering the
19 document, and can include means for negotiating a digital contract with the
20 registration server, the contract specifying licensing terms and auxiliary uses to the
21 work.

22
23 In still another aspect, a server is provided for managing digital copyrighted
24 works, including: (A) means for communicating with at least one on-line data
25 processor connected for communication with the server, the on-line data processor
26 having (i) means for recognizing a secure digital document having copyrighted
27 electronic media and minimum permissions data attached thereto, the minimum
28 permissions data specifying minimum authorized use of the media without a license
29 to the media; and (ii) means for opening the document and enabling a user of the
30 processor to use the media in accord with the authorized use; (B) means for

1 registering the document according to user-selected options at the data processor;
2 and (C) means for negotiating with the data processor to obtain auxiliary
3 permissions to the document and for sending the auxiliary permissions data to the
4 data processor thereby expanding the authorized use of the data processor.

5
6 The invention thus provides several advantages. By way of example, it
7 provides for identification of digital creative works so that potential licensees know,
8 or can learn of, the owner, author, creator, and publisher of the underlying digital
9 work. In accord with the invention, the use of the container, based in object
10 technology, with METADATA and the Digital Creative Work attached thereto
11 facilitates the appropriate identification of the Work. The METADATA provides the
12 vehicle for identification information and minimum permissions to the Work, and
13 further provides detail for subsequent licensing of the Work. Further, the invention
14 permits substantially seamless interaction between users and the Digital Creative
15 Work. By way of example, OBJECTs appear like any other visual instantiation on a
16 web page. It is only after the user tries to operate on the OBJECT beyond the user's
17 current consumption, e.g., viewing the OBJECT on the computer screen, when it
18 becomes apparent that there is additional control associated with the OBJECT.

19
20 The invention also provides for the secure electronic copyright management
21 and automatic identification of ownership of creative works distributed as digital or
22 electronic media, particularly over computer networks. Briefly, one aspect of the
23 invention provides a system which packages electronic media into a secure
24 document format (the "CONTAINER"), including a data container for the media
25 and a minimum permissions data set to specify the minimum authorizations needed
26 to view or otherwise access the media. The CONTAINER can also include a
27 container header, a container identifier, a source works extensions module which
28 maintains a bibliographical history of the media, and a digital signature to
29 authenticate the media. The CONTAINER and the associated network-based tools,
30 described below and constructed according to the invention, enable the attachment

1 of minimum permissions to copyrighted works and the subsequent on-line licensing
2 of the media.

3
4 More particularly, and in another aspect of the invention, the CONTAINER
5 containing the media is registered on a registration server and licensed through an
6 authorization server (together the "REGISTRY"). Potential licensees view the
7 CONTAINER through the authorizations within the minimum permissions data set,
8 and communicate with the authorization server, if desired, to obtain a license to the
9 media. Once licensed, the licensee can utilize the media in accord with an auxiliary
10 permissions data set that is assigned to the CONTAINER during the on-line
11 licensing transaction.

12
13 Subsequent viewers and/or users of the CONTAINER also communicate
14 with the authorization server. Thus, in another aspect, the invention provides for the
15 licensing of the media to creators of derivative works, i.e., those who modify an
16 original work of authorship and who obtain authorization to do so through an
17 augmentation in the permissions data set. As above, the modified CONTAINER is
18 then registered on a registration server and licensed through an authorization server.
19 The CONTAINER in this aspect preferably includes a sourceworks extension
20 module which records the original and derivative authorship of the media. By
21 retaining such information, a copyright "family tree" or electronic bibliographic
22 record is maintained for the media. Preferably, the authorship information in the
23 sourceworks extensions is resident as a data element within the CONTAINER.
24 However, the sourceworks extensions can also be maintained on or through the
25 authorization servers, depending upon the number of servers used in the
26 registration of derivative uses of the media.

27
28 Like the sourceworks extensions, the invention can also record any and all
29 users who access the media. In accord with this aspect, the CONTAINER includes a
30 usage module which records selected information about each user who accesses the

1 media. The selected information can include, for example, a unique address of the
2 user, individual or company accessing or utilizing the media, or the actual identity
3 of the user. Preferably, the user information stored in the usage module is recorded
4 and stored only after auxiliary permissions are augmented to the minimum
5 permissions data set; and typically, the user's identity or location is recorded in the
6 course of the licensing transactions with the authorization server. Like the
7 sourceworks extensions, the usage module can also be resident with the
8 CONTAINER, as another data element, and/or with the authorization server. In the
9 latter case, each time a user communicates with an authorization server to license a
10 particular media, the user's identity or location are recorded and stored therein.

11
12 Accordingly, the invention provides several advantages in the automation
13 and tracing of copyright clearances for both the initial users and derivative
14 developers of electronic media. Unlike the methods in the prior art - i.e., the method
15 of relying on copyright laws and treaties to protect copyrighted works, and the
16 method of encrypting the media through electronic keys - the CONTAINER format
17 and system architecture of the invention provide for (1) both fair use and ownership
18 protection; and for (2) automatic management of media rights, including the
19 controlled access to media in derivative works. Specifically, the system of the
20 invention attaches certain minimum permissions to a widely-distributed version of
21 the media packaged as a CONTAINER, thus being generally usable for free personal
22 use. The CONTAINER creator or author determines these minimum permissions in
23 the spirit of fair use, and the permissions data set are subsequently updated to an
24 auxiliary permissions data set through on-line licensing should the user be
25 interested in more advanced licensing or uses of the media.

26
27 In other aspects, the invention provides an encrypted electronic signature and
28 optional data encryption, to enhance or guarantee the authenticity of the entire
29 work, including authorship. More particularly, in other aspects, the CONTAINER

1 encapsulates the required data in a secure fashion using encryption; and the digital
2 signatures are based on message digests resulting from one-way hash functions.

3
4 In still other aspects, the system of the invention utilizes client/server system
5 architecture based upon the TCP/IP network protocol standard. Those skilled in the
6 art will appreciate that other network protocol standards can be used without
7 departing from the scope of the invention.

8
9 In accord with further aspects of the invention, users can unpackage or
10 unwrap CONTAINERS through a controlled environment, specifically from within a
11 compatible application or program extension, i.e., a Plug-in, which can provide the
12 requisite controls over document use.

13
14 The invention also provides a set of easy-to-use network-based tools for
15 registering and administering copyrights of electronic creative works. In one aspect,
16 for example, a viewing module is provided to view and edit media-packaged
17 graphic, image, video, audio, and textual objects. This viewing module, referred to
18 herein as a "VIEWER," is generally required, along with the SYSTEM EXTENSION,
19 to view and edit Digital Creative Works within CONTAINERS.

20
21 In still another aspect, a packaging module is provided to encapsulate a
22 newly created work in a secure, digitally-formatted package - i.e., a CONTAINER.
23 The packaging module, referred to herein as a "PACKAGER," is particularly useful
24 to authors, creators and publishers who seek to secure their copyrighted works and
25 who seek to encapsulate other information with the works, such as authorship,
26 ownership, minimum permissions, and source works extensions. Accordingly, a
27 user of the PACKAGER can selectively package such information with the media to
28 formulate a CONTAINER.

29

1 In other aspects, a registration server provides registration and authorization
2 services on a platform such as Windows NT or Unix. The registration server is used
3 by information creators who want users of their works to easily identify ownership
4 and potential licensing terms, and to transact and license those works on-line. The
5 Authorization server, on the other hand, is used by information creators and users to
6 obtain access to Digital Creative Works and to license those works for their own use.
7 Typically, in accord with another aspect, the registration server for each
8 CONTAINER operates as the authorization server for all subsequent licensing
9 transactions to that CONTAINER. In this latter aspect, the combination registration
10 server and authorization server is a REGISTRY.

11

12 The invention provides certain other advantages over the prior art in that
13 creators and publishers of electronic media have direct control of the copyrights they
14 hold through the use of authorization and registration servers. Further, the
15 invention is preferably compatible with widely accepted object technology
16 standards, e.g., OLE and OpenDoc, to ensure compliance with the widest possible
17 range of applications and on several platforms.

18

19 The invention also provides for automated and controlled network-based
20 copyright management. The registration server can be scaled to fit the needs of any
21 authorization and registration service, from single-author shops to massive
22 centralized clearinghouses.

23

24 In still another aspect, the VIEWER provides a mechanism for users to gain
25 access to the data within copyrighted CONTAINERS. Specifically, the VIEWER and
26 SYSTEM EXTENSION ensure that operations performed on media-packaged data
27 objects are in compliance with the permissions that have been granted to the user.

28

29 In other aspects, a user can transact a license to the CONTAINER through on-
30 line communications with the REGISTRY. More particularly, the SYSTEM

1 EXTENSION in this aspect (i) generates a licensing request signal in response to
2 inputs by the user, and (ii) communicates that signal to the authorization server
3 assigned to that CONTAINER. This request, sometimes denoted herein as a "License
4 Request," provides an entry point for on-line licensing of media-packaged works. In
5 this way, a successfully licensed user can obtain auxiliary permissions to the
6 CONTAINER of interest, thereby extending the set of operations which the user may
7 perform for a given work.

8
9 In still other aspects, the SYSTEM EXTENSION operates to display selected
10 registry information about the CONTAINER. This display, sometimes denoted
11 herein as the "Registry Information Display," provides information such as
12 authorship, ownership, and the licensing terms associated with the electronic media,
13 thereby facilitating the user's review and evaluation of the CONTAINER prior to
14 licensing. The registry information is preferably stored in the CONTAINER itself,
15 and/or at the CONTAINER's registration server.

16
17 A record of the media source works is also available through the SYSTEM
18 EXTENSION, in accord with another aspect of the invention. As discussed above,
19 the sourceworks extensions provide a bibliography of the authors of the media so
20 that the appropriate authors are credited with their works even after the works are
21 edited by a derivative author. The sourceworks extensions are typically available
22 within a display - sometimes denoted herein as the "Source Works Display" - at the
23 user's computer terminal.

24
25 In accord with other aspects of the invention, the SYSTEM EXTENSION
26 provides standardized tools and procedures for obtaining a certified digital
27 identification of a CONTAINER, and for becoming a licensed user to that
28 CONTAINER.

29

1 In another aspect of the invention, a PACKAGER encapsulates authorship,
2 ownership, minimum use permissions, source works information and the associated
3 creative works in a secure package. The PACKAGER has several aspects, including:
4

- 5 • Through the PACKAGER, a user can display the status of permissions for
6 each source work, obtain authorship, ownership, and licensing
7 information from the source work's registration server, and selectively
8 obtain auxiliary permissions as required for each source work.
 - 9 • The PACKAGER allows the author to check clearances for all sources of a
10 work in progress and to engage in EXTENSION-like licensing transactions
11 to obtain or upgrade auxiliary permissions.
 - 12 • The PACKAGER allows the author to verify and modify the information
13 that is encapsulated with the packaged media in a CONTAINER.
 - 14 • Registration is the final step in setting up a CONTAINER in accord with
15 the invention; and the PACKAGER provides a registration client and
16 procedure for registering a new creative work.
 - 17 • Like the SYSTEM EXTENSION, the PACKAGER provides standardized
18 tools and procedures for obtaining a certified digital identification and for
19 becoming an authorized user.
- 20

21 In another aspect of the invention, a Software Development Kit (SDK) is
22 provided to enable developers of multimedia applications, games, or multimedia
23 authoring tools (including applications for content creation) to incorporate VIEWER,
24 SYSTEM EXTENSION and PACKAGER functionality into their applications.
25

26 The invention thus facilitates the management of copyrighted works and
27 ensures that the media packaged within a CONTAINER is authentic. The invention
28 further enables the packaging of useful and selective information with the creative
29 work, such as container identification, ownership, permissions, and sourceworks
30 extensions. These features are provided, at least in part, by the VIEWER, SYSTEM

1 EXTENSION, PACKAGER and the REGISTRY. Through the registration server, for
2 example, information providers of any size can take advantage of rights
3 management for their creative works, and users on a network connected to the
4 server enjoy easy and secure on-line licensing of the works managed therein.

5
6 In accord with a preferred aspect of the invention, the VIEWER, SYSTEM
7 EXTENSION and PACKAGER do not impose perceivable overhead during the
8 course of normal rendering or editing of the work. The execution of VIEWER,
9 SYSTEM EXTENSION and PACKAGER functionality is quick to ensure that
10 network functions have good performance within the available network bandwidth.

11
12 In still other aspects of the invention, VIEWER, PACKAGER, Registration
13 Server Modules and Authorization Server Modules are operable on Win95,
14 Windows NT, MacOS and Unix-based platforms.

15
16 In other aspects, the VIEWER, SYSTEM EXTENSION and PACKAGER of the
17 invention operate in conjunction with OLE and OpenDoc.

18
19 The invention also provides a system for authorizing access to copyrighted
20 electronic media. An authorization server is connected for data transfer between an
21 internal memory and at least one external data processor, and an internal storage
22 stores selected information about the electronic media, e.g., the licensing terms for
23 gaining auxiliary permissions to the media, the copyright ownership of the media,
24 and revenue estimates about the media. A relay section that is responsive to a
25 request signal by the data processor communicates the selected information to the
26 data processor. A data comparison section receives response signals from the data
27 processor and compares the selected information with the response signals. In this
28 way, the data comparison section generates an acceptance signal when the response
29 signals correspond to at least a part of the selected information, and communicates
30 the acceptance signal to the data processor to authorize access to the media.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

The system can also store the media within a storage memory, in another aspect. This memory can be within a computer connected for electronic data transfer with the data processor, whereby the computer is responsive to the acceptance signal to transfer either (1) authorizations to access the media or (2) the media to the data processor.

The system preferably includes a process section for tagging an encrypted digital signature to the media, thus authenticating the media. Another section - including a source works extension module - can also be included to append a bibliographic record to the media, the bibliographic record forming a digital representation that specifies information that references each source work and access restrictions associated with the source work.

The system can further include a section for appending auxiliary permissions to the media, the auxiliary permissions forming a digital representation that specifies an authorized use of the media, such as viewing, copying or editing the media.

In yet another aspect, the system includes an access control section for withholding access authorization to a portion of the media, the access control section thus being responsive to the acceptance signal to remove access restrictions to the portion. In this way, permissions and access to copyrighted media can be provided to specified parts of a complex multimedia object, e.g., one which includes written text, graphics and sounds.

The invention further provides a system which controls selective access to electronic media. The system includes one or more servers that communicate via a data transfer link between an associated system memory containing the media and at least one external data processor. A communication section communicates content-specific permission information about the media to the data processor, the

1 permission information specifying data processor actions which are restricted and
2 which require augmented access privileges to perform. A storage section enables the
3 storage of selected other information about the media; while a relay section,
4 responsive to a request signal by the data processor, communicates the other
5 information to the data processor. A data comparison section receives response
6 signals from the data processor and compares the other information with the
7 response signals, the data comparison section generating an acceptance signal when
8 the response signals correspond to at least a part of the other information. An access
9 section restricts data transfers between the data processor and a portion of the
10 media, the access section being responsive to the acceptance signal to remove data
11 transfer restrictions between the data processor and the portion within the system
12 memory.

13
14 The communication section of this aspect can include one of (i) a stand-alone
15 software module, (ii) a plug-in software module corresponding to an application
16 environment that generated or modified the media, (iii) a program extension
17 corresponding to an application environment which generated or modified the
18 media, (iii) a software module integrated into an application environment by way of
19 a source code library or linkable object code performing substantially similar
20 functions.

21
22 Although other communication protocols are suitable for the invention,
23 communication standards based upon the TCP/IP network protocol are preferred.

24
25 The invention also provides methods for authorizing data transfers of
26 copyrighted digital media, including: affixing content-specific permission
27 information to the media, the permission information specifying actions which are
28 restricted and which require augmented access privileges to perform; storing
29 selected information about the electronic media on an authorization server
30 connected for data transfer with at least one computer; electronically

1 communicating selected information about the media to the computer; receiving
2 response signals from the computer and comparing the selected information with
3 the response signals; and generating an acceptance signal when the response signals
4 correspond to at least a part of the selected information, thereby authorizing access
5 to the media.

6

7 The invention also provides for optional encryption of the data within the
8 secure container. Accordingly, the methods of the invention include, for example,
9 the step of encrypting the media through an RSA public key algorithm.

10

11 The method of this aspect can also include the step of communicating a
12 digital representation of at least one of (i) a copyright ownership of the media, (ii) a
13 set of licensing terms for the media for different user classifications, and (iii) revenue
14 estimates about the media.

15

16 In another aspect of the invention, a method is provided for maintaining an
17 electronic bibliographic record of digital media, including: opening an object
18 container containing the digital media, the object container including a
19 representation of the media, a data identifier of media, and data specifying
20 minimum permissions required to access the media; editing the digital media in an
21 application environment; and attaching the data identifier and minimum
22 permissions data to the edited media into a source works list. The source works list
23 provides, among other information, a bibliographic record of the authorship
24 represented in the media.

25

26 Such a method can also include the steps of decrypting the media, and
27 encrypting the media after attaching the data identifier and permissions data into
28 the source works list.

29

1 A method of the invention also includes a process for determining the
2 authenticity of digital media, including the step of affixing an encrypted digital
3 signature to the media. In this aspect, the CONTAINER is authenticated by encoding
4 a signature representing the registration of the media. By way of example, a private
5 key is resident with the registration server which is under strict control of the
6 system. The authenticity - in this example - is thus granted by the registration server
7 and proven by the digital signature in the CONTAINER. Alternatively, in another
8 example, the private key is provided to the user of a particular application, again
9 under the tight control of the system.

10
11 In yet another aspect, a computer network is provided for managing original
12 works of authorship, including: a process actuation section for affixing copyright
13 information to a binary data element corresponding to an authored media; a process
14 actuation section for affixing minimum permission information to the data element,
15 the permission information specifying access restrictions to the data element; a
16 server for storing information concerning the rights to the media, the server
17 including a control module for controlling access to the data element according to
18 the minimum permission information by restricting data transfers between the
19 server and one or more computers networked with the server; a process section for
20 tagging the data element with supplemental information; and a process section for
21 maintaining copyright information through derivative uses of data element
22 throughout the network.

23
24 The invention also provides a PACKAGER, which is a system for packaging
25 electronic media within a secure electronic container. The PACKAGER includes a
26 first process section for attaching a data identifier to the media; and a second process
27 section for attaching minimum permissions data to the encrypted media, the
28 minimum permissions data specifying minimum acceptance terms required to
29 electronically access the media.

1
2 In other aspects, the PACKAGER includes a process actuation section for
3 attaching a digital signature to the media, the digital signature providing an
4 authentication to the media; and a process actuation section for affixing source
5 works extensions to the media, the source works extensions specifying a
6 bibliographic record of the media. This bibliographic record is a digital
7 representation that specifies bibliographic information about the authors and
8 minimum permissions of the media, thereby providing persistence through
9 generations of derivative use of the media.

10
11 A SYSTEM EXTENSION and VIEWER subsystem is also provided for
12 unpackaging electronic media configured within a secure electronic container. A
13 first process actuation section recognizing permissions data attached to the media,
14 the permissions data specifying one or more authorizations needed to electronically
15 access the media; and a second process actuation section opens the media when a
16 user has the authorizations corresponding to the permissions data.

17
18 In other aspects, the subsystem includes a communication section that
19 engages an authorization server when the user does not have the requisite minimum
20 authorizations of the permissions data set; or when a user desires to augment the
21 permissions to a particular media by transacting a license to that media. The
22 communication section thus includes a process section for transmitting transactional
23 information to the server, and for receiving, from the server, auxiliary permission to
24 utilize the media.

25
26 The methods of the invention can include the steps of encrypting the media,
27 and/or transferring the container to the data processor via one of point-to-point
28 email, CD-ROM, ftp, gopher, smtp (email), and http (World Wide Web). In one
29 aspect of the invention, for example, the registration server first authorizes a user
30 with a PACKAGER through log-in process to establish a secure line, such as known

1 in the art. The user and PACKAGER then generate the registration information
2 relating to the particular CONTAINER, and transmit the information and a message
3 digest to the registration server. Upon receipt, the registration server returns a
4 "registration certificate," in digital form, that is signed by the server's private key.
5 The registration server's public key is widely known, so that the registration server
6 can operate as a certification authority for the packaged-media. The registration
7 certificate is then passed through secure channels, and the PACKAGER attaches the
8 digital signature to the CONTAINER. Accordingly, authenticity is demonstrated to
9 anyone with a VIEWER or PACKAGER that has access to the CONTAINER.

10
11 In an alternative aspect, if the communication channel is unsecured, the
12 registration certificate is encrypted via public key to the user's public key.

13
14 These and other aspects and advantages of the invention are evident in the
15 description which follows and in the accompanying drawings.

16
17 Brief Description of the Drawings

18
19 Figure 1 illustrates one system, constructed according to the invention, for
20 managing copyrighted works formed as CONTAINERS;

21
22 Figure 1A illustrates a schematic view of one CONTAINER constructed
23 according to the invention;

24
25 Figure 2 shows a schematic illustration of a VIEWER and SYSTEM
26 EXTENSION subsystem, constructed according to the invention, and which is
27 suitable for viewing selected information within a CONTAINER such as illustrated
28 in Figure 1A;

1 Figure 3 shows a schematic illustration of a PACKAGER system, constructed
2 according to the invention, and which is suitable for encapsulating electronic media
3 within a CONTAINER such as illustrated in Figure 1A;

4
5 Figure 4 illustrates a schematic diagram of a system which is constructed
6 according to the invention and which provides for managing copyrighted electronic
7 media assets;

8
9 Figure 5 shows one illustrated use of the invention in the management of
10 copyrighted GIF files;

11
12 Figures 5a and 5b show illustrative dialog boxes displayed to a user of the
13 system of Figure 5;

14
15 Figure 6 shows a computer network constructed according to the invention and
16 which illustrates selected operational uses of the invention;

17
18 Figures 7-7h show illustrative computer displays for use with a system
19 constructed according to the invention, such as the network of Figure 6;

20
21 Figure 8 illustrates one acceptable process flow for providing copyright
22 management according to the invention;

23
24 Figure 9 schematically shows a system, constructed according to the invention,
25 and which illustrates selective operations of a VIEWER, SYSTEM EXTENSION,
26 PACKAGER and registration/authorization server;

27
28 Figure 10 illustrates various components of the invention, including a
29 CONTAINER, REGISTRY, OBJECT, SYSTEM EXTENSION, MATADATA, DIGITAL

1 CREATIVE WORK, VIEWER, PACKAGER, TOOLBOX, DIGITAL CONTRACT; and
2 further illustrates certain relationships between such components;

3
4 Figure 11 illustrates a system, constructed according to the invention, for
5 managing digital creative works, and shows one operational interaction between a
6 CONTAINER, REGISTRY, SYSTEM EXTENSION and TOOLBOX;

7
8 Figure 12 schematically illustrates interaction between a
9 PACKAGER/TOOLBOX, Registration Server, and SYSTEM EXTENSION, in accord
10 with the invention;

11
12 Figure 13 schematically illustrates one packaging process flow in accord with
13 the invention;

14
15 Figure 14 shows a representative property page template constructed according
16 to the invention;

17
18 Figure 15 illustrates a template overlaid onto an OBJECT that instantiates a
19 CONTAINER constructed according to the invention; and

20
21 Figure 16 schematically shows a registration server system constructed
22 according to the invention.

23
24 Detailed Description of the Invention

25
26
27 Figure 1 illustrates a system 10, constructed according to the invention,
28 whereby CONTAINER 12a, 12b are created and packaged, and then registered on
29 associated registration servers 14a, 14b, respectively. Users 16a, 16b and 16c are
30 connected for data transfers with one or more of the authorization servers 18a, 18b,
31 such as through a computer network or the Internet.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

The illustrated CONTAINERS 12a, and 12b are created as copyrighted media by author 19 and user 16a, a derivative author of the work 12a. For example, media 13 is representative of original work of authorship. Thereafter, the CONTAINERS 12a, 12b are packaged as a data container, according to the systems and methods described herein, and as denoted by the copyrighted © symbol marked over the media. These packaged CONTAINERS 12a, 12b are registered on servers 14a, 14b, respectively, and are made available for license through authorization servers 18a, 18b. A single server can operate as both the registration server and authorization server.

In operation, the CONTAINERS 12a, 12b are available for limited free use according to the minimum permissions data set assigned to each CONTAINER. Typically, the minimum permissions allow users with access to the CONTAINER to view the CONTAINER, but not to save or otherwise transfer the CONTAINER without first obtaining auxiliary permission from the CONTAINER's authorization server. As illustrated, for example, users 16a, 16b each have access to CONTAINER 12a and may therefore freely read or view the contents of the media within CONTAINER 12a at their associated personal computers 17a, 17b, respectively. If, however, the users 16a, 16b attempt to act on the CONTAINER 12a in a manner which is not in accordance with the permissions they hold, they are automatically prompted to obtain a license to the CONTAINER 12a. The licensing transaction occurs through the authorization server 18a, which connects and communicates with the users 16a, 16b through personal computers 17a, 17b. Alternatively, the users 16a, 16b may, if desired, initiate a licensing transaction with the server 18a if they know, for example, that their permissions are insufficient to access the CONTAINER 12a in the desired way.

Once licensed to the CONTAINER 12a, the licensed user has augmented auxiliary permissions to utilize the CONTAINER in some other way, such as saving

1 and/or modifying the CONTAINER. Similarly, user 16c is connected via computer
2 17c to the authorization server 18b, and may therefore view and, if desired, license
3 CONTAINER 12b through server 18b. The format of CONTAINERS 12a, 12b are
4 described in more detail in connection with Figure 1A.

5
6 CONTAINER 20 of Figure 1A provides a secure container for electronic
7 media, including heterogeneous multimedia data types such as musical scores
8 coupled with graphical images. More particularly, the CONTAINER 20 provides a
9 package that encapsulates binary data objects, shown as the data container 23, and
10 can contain some or all of the illustrated data components 21, 22, 24, 25 and 26.

11
12 In Figure 1A, the Container Header 21 contains basic information about the
13 CONTAINER 20, including, without limitation, information such as a unique file
14 format identifier, a format revision code, a document creator application type, a file
15 type (typically the MIME type code) of the enclosed data, a comment field length,
16 and a comment field, typically up to about 256 characters. The information within
17 Container Header 21 is generally not encrypted.

18
19 The Container Identifier 22 uniquely identifies the CONTAINER 20 by the
20 registration server upon which the CONTAINER has been registered, and the
21 CONTAINER's registration or index number on that server. This registration code
22 typically contains the server name and registration index. A registration server cross-
23 reference table, working in conjunction with the Internet's Domain Name Service
24 (DNS), is used to find the actual network address (typically a TCP/IP address) of the
25 registration server. In one example, a unique server code may indicate local
26 registration, usually indicating a work in progress. In another example, an author
27 logged onto a computer, such as the author 20 of Figure 1, and actively generating a
28 copyright work in progress, e.g., a novel in Microsoft Word™, will update and store
29 the work on the local computer. In one embodiment of the invention, a work in

1 progress is a locally accessible file which has not been authenticated through the
2 registration process.

3
4 The Data Container 23 contains the information representing the electronic
5 media or Digital Creative Work, typically in an original file format. If desired by the
6 author, this data can be secured through encryption, such as through secret or public
7 key methods known in the art. The data within the Container 23 is usually passed in
8 the clear, i.e., unencrypted. However, increased control can be obtained through
9 encryption of the associated media. The fields within the Data Container 23 can
10 include the enclosed data file, and can include the data container extension code,
11 and the data container size, among other information.

12
13 The Source Works Extensions 24 provides a bibliographic record, or
14 'persistence,' of copyright uses through generations of derivative work. The data
15 fields within the Sources Works Extensions 24 can include any of the Source Works
16 Extension Code, the Container ID, and the Permissions mask. If demanded by the
17 licensor of the work, or desired by the licensee, the Container ID and the applicable
18 permissions mask (the set of relevant use permissions) for the source work are
19 included in the derivative work. In accord with the preferred use of the invention,
20 the Source Works Extensions 24 are encrypted; and any number of Source Works
21 Extensions 24 may be included in a CONTAINER 20. For example, information
22 about successive derivative authors of the CONTAINER 20 are stored sequentially
23 as a Source Works Extension 24. By way of another example, one Source Work
24 Extension 24 can include the release information for any performer whose image or
25 audio likeness appears in the current CONTAINER.

26
27 The Source Works Extensions preferably operates to protect the source works
28 author, even at the risk of burdening the derivative author and/or developer.
29 Authors can require that their work is included as a source works extension in a
30 derivative work, or they can leave this choice to the editor or derivative developer.

1 Authors can also request that their source works are not displayed. For example,
2 they may require the derivative developer to go through the authorization process
3 again to obtain permissions and to include information regarding the work.
4

5 The Minimum Permissions 25 includes a permissions data set that are
6 distributed with all authentic copies of the CONTAINER 20. These permissions
7 affect the minimum use of the data within the Data Container 23 in cases where an
8 on-line licensing transaction has not yet taken place. The Minimum Permissions 25
9 thus uphold the spirit of the fair use doctrine of copyrighted works; and the careful
10 setting of the minimum permissions data set by the author(s) or creator(s) of the
11 media ensures easy access and limited free use of the media up to the minimum
12 authorized permissions set forth in the Minimum Permissions 20. This free use
13 through minimum permissions is made possible by viewing the CONTAINER 20
14 through a SYSTEM EXTENSION, constructed according to the invention and
15 described in more detail below, which is widely distributed to potential users of the
16 CONTAINER 20.
17

18 Minimum permissions 25 are superseded by auxiliary permissions which are
19 assigned to the CONTAINER 20 during an on-line licensing transaction. Auxiliary
20 permissions are preferably contained in secure License Certificate documents
21 provided by the Registration Server and encrypted to the licensee's key.
22

23 In accord with the preferred embodiment of the invention, an encrypted
24 Digital Signature 26 is also part of the CONTAINER 20, to facilitate authentication.
25 While the Signature 26 can be encrypted to ensure the authenticity and integrity of
26 the CONTAINER 20, encryption of the bulk data 23 is also possible to guarantee a
27 higher level of security.
28

1 Those skilled in the art will appreciate that other orderings of the information
2 within the CONTAINER 20 are possible, including one where the Data Container 23
3 is last.

4
5 In accord with the preferred embodiment of the invention, users can
6 unpackage or unwrap the CONTAINER 20 only through the controlled management
7 of the copyrights associated with the CONTAINER 20. Specifically, the
8 CONTAINER 20 is viewable through the SYSTEM EXTENSION and, if needed, a
9 VIEWER. The VIEWER is available in several formats to accommodate the differing
10 types of media contained within the CONTAINER. By way of example, once the
11 CONTAINER 20 is recognized by the SYSTEM EXTENSION, documents formatted
12 within the Data Container 23 of Figure 1A can be opened and manipulated on
13 compatible applications such as:

- 14
- 15 • Stand-alone VIEWER applications, with SYSTEM EXTENSION functionality
16 provided therein, which allow viewing of the media and of the networked
17 licensing and registration information.
 - 18 • Applications which are fully OLE compliant and where the OLE2
19 implementations of the SYSTEM EXTENSION, VIEWER and PACKAGER
20 reside on the system.
 - 21 • Applications for which VIEWER and/or SYSTEM EXTENSION plug-ins may
22 be available, so that user's of applications such as Adobe's Photoshop®,
23 Premiere®, and Acrobat® can directly interface with CONTAINERS.
 - 24 • Applications with integrated kernel software encompassing VIEWER and
25 EXTENSION-like functionality, such as for integration into World Wide Web
26 software like Mosaic® and Netscape®.
- 27

28 The CONTAINER 20 of Figure 1A can also include information about the
29 successive users of the CONTAINER. For example, the Source Works Extensions 24
30 can have an appended data field or usage module which stores selected information

1 about the users of the CONTAINER. Such usage information can include, for
2 example, the identity and/or location of the user. Alternatively, the usage
3 information can be stored at the associated authorization server during or in
4 connection with a licensing transaction to the CONTAINER.

5
6 In summary, the CONTAINER format of Figure 1A augments the
7 multimedia data content with supplementary information which identifies, without
8 limitation, some or all of the following information: the source, registry, and format
9 of the data; the copyright legacy of the data; minimum permissions to use of the data
10 prior to on-line licensing; a digital signature to prove authenticity of the data; and a
11 use record of the users who accessed the media.

12
13 Figure 2 illustrates a VIEWER and SYSTEM EXTENSION combination system
14 30 constructed according to the invention and which is suitable for viewing the
15 CONTAINER 20 illustrated in Figure 1A. The system 30 includes a series of process
16 actuators 32a...32f, each of which decodes and/or interprets the several elements of
17 the CONTAINER 20. The system 30 is connected for data transfer along data
18 transfer line 34 to communicate and operate on the CONTAINER 36, stored for
19 example on a server. The several process actuators 32 thereafter operate, in
20 combination, to enable viewing of the media within the CONTAINER 36 and in
21 accord with the minimum permissions data set. This media is illustrated in Figure 2
22 as the data objects 38, which are, for example, displayed in a computer screen,
23 through data transfer line 34a, so that a user can view the contents of the media data
24 objects.

25
26 The system 30 can be constructed as a printed circuit board, application
27 specific integrated circuit, a VLSI circuit, or as a software module resident within a
28 computer and operable in connection with an internal microprocessor to perform the
29 various process actuator functions described below in connection with process
30 actuators 32a...32f. Typically, the system 30 is connected for communication with a

1 computer display so that once the CONTAINER 36 is unpackaged, the data objects
2 38 within the CONTAINER 36 are viewable to the user.

3
4 More particularly, the process actuator 32a interprets selected information
5 about the container header, e.g., the header 21 shown in Figure 1A. This information
6 can, for example, include the type of file within the CONTAINER 36, or a comment
7 field specifying certain details about the media as described by the media's author.
8 Process actuator 32b, likewise, interprets selected information about the container
9 identifier, e.g., the identifier 22 of Figure 1A. Such identifier information includes, at
10 least, a unique identifier of the registration server upon which the CONTAINER 36
11 is registered, so that appropriate on-line licensing transactions can occur with the
12 appropriate location. Process actuator 32c interprets - and sometimes decrypts - the
13 data formulating the media 38, so that the user can view the media 38 to evaluate
14 whether to engage in a licensing transaction. The process actuator 32c provides
15 minimum access to the media 38 in accord with the minimum permissions data set
16 which is associated with the CONTAINER 36 and which is loaded and interpreted
17 by the actuator 32d. Process actuator 32e interprets selected information about the
18 source works extensions associated with the CONTAINER 36, while process
19 actuator 32f interprets information about the digital signature associated with the
20 CONTAINER 36, thereby providing a means to authenticate the media 38.

21
22 Not all process actuators 32 are required in every system 30, depending upon
23 the form of the CONTAINER 36. At a minimum, however, the system 30 must be
24 able to interpret the data within the CONTAINER, including, if necessary, decrypt
25 algorithms needed to unlock any encrypted data within the CONTAINER 36; and
26 the system 30 must identify the CONTAINER's minimum permissions as well as the
27 connectivity information of the CONTAINER's associated authorization or
28 registration server. The system 30 will not, however, typically permit further
29 actions - such as copying and/or downloading of the media 38 to disk - without first
30 obtaining auxiliary licensing permissions from the associated authorization server,

1 as described in more detail below. The system 30 thus provides a minimum access
2 to the data 38, such as viewing the media contents on the user's display terminal,
3 thereby promoting limited but fair use of the data 38.

4
5 Similarly, electronic media is packaged into a format such as the
6 CONTAINER 20 through a packager system constructed according to the invention
7 and denoted herein as a PACKAGER, such as illustrated in Figure 3. The
8 PACKAGER system 40 of Figure 3 is suitable for generating the CONTAINER 20
9 illustrated in Figure 1A. The PACKAGER 40 includes a series of process actuators
10 42a...42f, each of which operates to formulate one or more of the elements of the
11 CONTAINER 20, Figure 1A. The PACKAGER 40 is connected for data transfer
12 along data transfer line 44 to communicate and operate on electronic media 46. The
13 several process actuators 42 thereafter operate in combination to package or
14 encapsulate the media 46 into a secure CONTAINER 48. For example, a user of the
15 PACKAGER 40 is generally an author of copyrighted works, and one process
16 actuator is used to specify the minimum authorized use of the media within the
17 minimum permissions data set. The resulting packaged media, illustrated in Figure
18 3 as the CONTAINER 48, is thereafter registered on a registration server, through
19 data transfer line 44a, so that the CONTAINER 48 is available for on-line licensing
20 transactions by any connected user having a SYSTEM EXTENSION and connected to
21 the authorization server.

22
23 By way of example, the PACKAGER 40 can be constructed as a printed circuit
24 board, an application specific integrated circuit, a VLSI circuit, or as software
25 module resident within a computer and operable in connection with an internal
26 microprocessor to perform the various process actuator functions described above in
27 connection with process actuators 42a...42f. Typically, the PACKAGER 40 is
28 connected for communication with a registration server so that once the
29 CONTAINER 48 is packaged, the data objects 46 within the CONTAINER 48 are
30 available for license by any connected user.

1
2 Sufficient information is packaged within the document format to enable a
3 potential licensee using the SYSTEM EXTENSION to engage in on-line licensing
4 transactions to obtain, for example, copyright ownership, licensing, and revenue
5 information about the data. If the terms are acceptable, the potential licensee uses the
6 SYSTEM EXTENSION to obtain additional permissions for derivative development
7 or other use not covered in the minimum permissions data set. This operation is
8 described below in connection with Figures 4-6.

9
10 Figure 4 illustrates a copyright management system 50 constructed according
11 to the invention. Specifically, Figure 4 illustrates how copyright permissions will be
12 integrated into the multimedia production environment using the described
13 CONTAINER format. The media is first formulated as individual content elements
14 52 that are created and authored by media-specific tools, such as text editors,
15 graphics tools, audio design tools, and digital video production tools. In the
16 conventional production environment of the prior art, the elements 52 would simply
17 enter a multimedia asset library, ready for use in production. No copyright
18 information whatsoever would typically be affixed to the data objects prior to
19 archiving.

20
21 In system 50, on the other hand, content element-specific permissions are
22 affixed to each data object 52 before passing on to the next level of production or on
23 to archiving. In one embodiment of the invention, the system 50 incorporates a
24 PACKAGER 54 within a stand-alone application to affix permissions and other
25 related authorship information to the data 52, such as described in connection with
26 Figure 3. Alternatively, the PACKAGER 54 can be directly integrated into the media-
27 specific tools of the developers; and, as such, the PACKAGER 54 becomes a "plug-in"
28 tool for commercially available graphics, video, and sound development
29 applications based on the PACKAGER software kernel.

1
2 After packaging by the PACKAGER 54, the heterogeneous content elements
3 56 are registered on a registration server 58, and, for example, released to the
4 production library. During this stage of production, a multimedia authoring or
5 scripting environment can be used to create an interactive multimedia program
6 which is a composite of these archived elements 56. The control characteristics and
7 asset utilization of the program embodied in the control "script" may also have an
8 affixed permissions header. Thus all of the component assets will be protected in a
9 similar fashion.

10
11 For derivative uses of packaged CONTAINERS such as the packaged
12 elements 60 of Figure 4, a VIEWER and PACKAGER 62 can be utilized as a plug-in
13 to the associated application software which generated the media of CONTAINER
14 60 in the first place, so that editing and saving of the CONTAINER can occur. Such
15 modifications and saving correspond to a "derivative use," as described herein.
16 Once the works 60 are modified and packaged into a derivative CONTAINER 64,
17 including a Source Works Extension, they too are registered on a registration server
18 58 (illustrated as a single server, for ease of illustration) for future licensing
19 transactions, and, for example, released to a production library.

20
21 The system 50 thus provides an effective strategy for managing both in-house
22 and externally obtained copyrighted assets. In accord with one embodiment of the
23 invention, a two-tiered rights clearing scheme is provided for multimedia program
24 integration, in which both the encapsulated minimum permissions and the auxiliary
25 permissions of all incorporated works are reverified prior to compilation. The
26 specific content of this combination of permissions, including the permissions
27 introduced by the creator of the composite work, will dictate what sort of
28 authorization is required at execution time. Upon remote execution of the compiled
29 multimedia program, a spectrum of authorization schemes are possible, from free
30 execution, to the networked authorization of individual copyrighted assets. The

1 licensing functionality of the PACKAGER/VIEWER kernel is applicable during
2 execution as well as during production.

3
4 For illustrative purposes, Figure 5 shows a system 70, constructed according
5 to the invention, which only manages copyrighted GIF (graphics files) media. The
6 GIF CONTAINERS are created and/or modified through VIEWER and/or
7 PACKAGER systems, such as described herein, and are managed through a
8 registration server. Figure 5 shows, in particular, initial document processing, use-
9 based licensing, header and extension maintenance, source work copyright
10 clearance, local and remote server registration, and encrypted file formatting.
11 Preferably, the system 70 is based on TCP/IP.

12
13 The major functional sections of system 70 include opening files of
14 appropriate types, creating and modifying headers and extensions, providing
15 permissions clearance for included sources works and attached performance
16 releases, and CONTAINER formatting, encryption, and saving. Each of these
17 sections is described below:

18
19 Opening Files

20
21 CONTAINERS are loaded into the system 70 once packaged by a
22 PACKAGER. For example, an original work 72 created in an application
23 environment is opened in that environment and formatted by a PACKAGER into a
24 CONTAINER 74. Alternatively, an existing CONTAINER 76 can be opened by a
25 SYSTEM EXTENSION (and VIEWER if needed), modified if desired, and stored as a
26 CONTAINER 74.

27
28 More particularly, media is opened and available to the user through a
29 combination of the application which created the media (i.e., the VIEWER) and a
30 SYSTEM EXTENSION. In the case of raw GIF files, the images are displayed and a

1 header editing dialog box appears to the creator, such as shown in Figure 5a,
2 indicating that the system 70 is ready to start the formatting process. For
3 CONTAINER-formatted files, a dialog box appears listing basic information for the
4 main file, such as shown in Figure 5b; and similar information is listed in a scrolling
5 window for each of the Source Works.

6
7 The CONTAINER's minimum permissions (obtainable and resident, for
8 example, within any CONTAINER) and any auxiliary permissions (obtained from
9 an authorization server during a licensing transaction) will dictate how the opened
10 file may be used. To encourage browsing and fair use of CONTAINER-formatted
11 works, the publicly distributed CONTAINER files will typically have sufficient
12 minimum permissions to allow local viewing, at least, and sometimes unlimited
13 local derivative use. Publicly-distributed files which allow local viewing can be
14 opened by the SYSTEM EXTENSION (and VIEWER, if needed); and files which
15 require licensing to be opened, or working files which have not yet been publicly
16 registered, must be opened with the user's key.

17
18 Publicly distributed files are registered on a registration server, and if
19 encrypted, the key resident on the server is passed to the user via a secure channel.
20 Some of these files will require licensing at viewing time, meaning that auxiliary
21 permissions must be obtained. The auxiliary permissions files, or certificates, will be
22 encrypted based upon the registered user's key, as are works-in-progress (not
23 registered, and possibly with incomplete sources works clearance).

24 25 Creating & Modifying Headers & Extensions

26
27 System 70 has several interfaces for creating or modifying the headers and
28 extensions which embody the CONTAINER format. The Container Header, e.g., the
29 header 21 of Figure 1A, is primarily derived from attributes of the enclosed media
30 within the CONTAINER. These attributes are displayed in the DocInfo Editor and

1 Viewer windows shown in Figure 5a. The Container ID, e.g., the ID 22 of Figure 1A,
2 denotes the CONTAINER's registration server 78 and the index number of that
3 CONTAINER on that server. Non-local document IDs can only be assigned if there
4 is a valid registration certificate associated with the file. Local Container IDs are
5 encrypted, but can only be changed by the document owner. Container ID
6 maintenance is typically handled through a computerized dialog box.

7 8 Permissions Clearance and Source Works

9
10 For Source Works Extensions, e.g., the Extensions 24 of Figure 1A, the
11 Container ID information is displayed in a scrolling view for the set of source works
12 associated with the current file. A dialog box allows the CONTAINER IDs of
13 additional works to be specified. Permissions information can be obtained by
14 double-clicking an entry on this list. A transaction with the registration server 78 of
15 the source works 72, 76 may be initiated by selecting the appropriate CONTAINER
16 ID. Note that the user may choose to ignore clearances for locally-generated source
17 works.

18
19 To enable permissions clearance for source works, public registration will not
20 be permitted without proper source works clearance. This is ensured by the
21 following: first, system 70 will not allow on-line registration to take place unless the
22 permissions of the included source works (plus any auxiliary permissions) agree
23 with the intended minimum permissions and maximum licensable permissions, the
24 latter to be set at registration time. Secondly, the registration server 78 will not allow
25 registration unless it is proven that the source works are clear. Clearances are
26 required for those source works extensions with insufficient minimum permissions
27 for the intended distribution of the derivative work. These clearances are in the form
28 of auxiliary permissions, obtained on-line with licensing transactions identical to
29 those discussed earlier. Given the intended minimum and licensed maximum
30 permissions, the Source Works Manager Window displays those source works

1 whose permissions need upgrading. The user will then select each one individually
2 to launch a licensing transaction. Clearances that are encrypted are based on the
3 user's key, and therefore cannot be transferred.

4
5 Private works, or works-in-progress, may not require registration, but any
6 works which are to be publicly distributed — and, for example, encrypted using a
7 secret key — must be registered. Users must therefore demonstrate that all source
8 works in system 70 have been cleared prior to the registration attempt. Upon
9 successful registration, the user of system 70 will receive an encrypted registration
10 certificate which facilitates the saving of the CONTAINER in a publicly-viewable
11 form. Since registration and authentication is based on a unique message digest for
12 the file, if any changes are made to the file a new message digest must be calculated
13 and the CONTAINER's entry in the registration server database must be updated.

14
15 Encrypted data is preferably formatted with a secret key that is generated at
16 the encryption event, and transported using public key encryption.

17
18 Applications compatible with system 70 are preferably based on TCP/IP, and
19 therefore operate in the same manner as most popular Internet-compatible users.

20 21 Formatting, Encryption, & Saving

22
23 A PACKAGER of system 70 saves files in the CONTAINER format, such as
24 described above, and preferably encrypts the data therein. Exemplary encryption
25 schemes according to the invention include, without limitation:

- 26
27 • Encryption is initiated by the user, who also generates the secret key
28 which is passed to the server, by secure means, and which becomes part of
29 the registration record for that work. Upon the grant of auxiliary permissions,
30 the server passes the key to the licensed user as part of the certificate. This is

1 intended for publicly registered and distributed files, and a CONTAINER is
2 not encrypted in this way without being registered first.

3 • Encryption based on the author's key. All local works-in-progress may
4 be encrypted in this way, ensuring that local use is possible but unregistered
5 public use is not.

6 • Encryption based on another user's key. This permits collaboration
7 while protecting the collaborative work.
8

9 With further reference to Figure 5, once a CONTAINER 74 is saved and
10 registered on a server 78, it may be freely distributed. Derivative users 80 can gain
11 clearance to the CONTAINER 78 through the SYSTEM EXTENSION (and VIEWER,
12 if needed) and in accord with the minimum permission of the CONTAINER and the
13 auxiliary permissions from servers of all source works. The work 82 represents
14 either work in progress, or publicly available work; and can be encrypted, such as
15 described herein.
16

17 Figure 6 illustrates a computer network 90, constructed according to the
18 invention, for managing copyrighted electronic media. In a first instance, an original
19 author 92 generates and packages electronic media 93, e.g., such as described in
20 connection with Figure 3, and registers the CONTAINER 93 on registration server
21 94. Typically, the author 92 generates the work 93 on a computer that is connected to
22 the network via data transfer line 96. Once the author 92 registers the CONTAINER
23 93, the server 94 becomes an authorization server for any subsequent access and/or
24 licensing of the CONTAINER 93.
25

26 By way of example, user 96 has a VIEWER and is connected to the network 90
27 through communication line 97. The user 96 can thereby access the CONTAINER 93
28 through the authorization server 94 up to the minimum permissions data set forth in
29 the CONTAINER format. Typically, the minimum permissions permit viewing of
30 the CONTAINER; but do not permit saving and/or transmission of the

1 CONTAINER. Should the user so desire, he or she can license the CONTAINER
2 through an on-line licensing transaction with the authorization server 94 to obtain
3 additional authorizations - denoted herein as auxiliary permissions - to use the
4 media within the CONTAINER for some other use, e.g., saving or modifying the
5 CONTAINER.

6
7 Similarly, a Derivative User/ Author 100 of the CONTAINER can access and
8 modify the contents of the CONTAINER by first obtaining auxiliary permissions to
9 do so through the authorization server 94. More particularly, the author 100 first
10 views the CONTAINER via the SYSTEM EXTENSION (not shown) and VIEWER
11 and through the minimum permissions data set of the CONTAINER; then transacts
12 a license with the Authorization server 94 to obtain the auxiliary permissions. The
13 author 100 is thus connected via data transfer line 102 to the server 94; and has a
14 SYSTEM EXTENSION, VIEWER and PACKAGER resident at his computer (note, for
15 illustrative purposes, the Users and Authors 96, 100 and 120 of Figure 6 are shown
16 with limited detail; and generally include a computer with SYSTEM EXTENSIONS,
17 VIEWERs and/or PACKAGERs resident at the computer).

18
19 Once the derivative user 100 modifies the CONTAINER, the CONTAINER is
20 registered on registration server 104, through data transfer line 103, so that
21 subsequent licensing can occur by users such as user 110. Note that user 110 must
22 obtain licensing authorization from each server 104 and 94. This process is done
23 automatically at the user's computer terminal. The user 120 first accesses the
24 modified CONTAINER through the network 90 and by connection with the server
25 104 through data transfer line 105. Once the user 110 views the modified
26 CONTAINER, she can seek auxiliary permissions to use the data for her intended
27 use. Such auxiliary permissions are obtained by connecting to each of the servers 94
28 and 104 through data transfer lines 107 and 105, respectively.

29

1 Derivative author 112, connected to the server 104 via data transfer line 114,
2 operates a VIEWER and PACKAGER (and, if desired, a SYSTEM EXTENSION) in an
3 SDK environment. Briefly, the SDK indicates a "Software Development Kit" and
4 enables developers of advanced multimedia applications, games, or multimedia
5 authoring tools (including content creation applications) to incorporate System
6 Extension, Viewer and Packager functionality into their applications in advanced
7 ways. The SDK is appropriate, for example, when conventional OLE 2.0 compliance
8 does not deliver the functionality or performance that the ISV demands. As above,
9 the author 112 edits and creates multimedia works and packages them through the
10 PACKAGER resident in the SDK to provide for registration and subsequent
11 licensing of that work.

12

13 To maintain the authorship of, and ownership to a CONTAINER within the
14 network 90, sourceworks extensions are used. This extension can be resident within
15 the CONTAINER, such as shown in Figure 1A, so that the appropriate CONTAINER
16 authorship and/or ownership is recorded and stored in the appropriate data
17 element within the CONTAINER. Alternatively, or concurrently, the sourceworks
18 extension is stored on any and all of the servers 94 and 104. In this way, the owner or
19 authors of the CONTAINER can ensure persistence through generations of
20 derivative use. Further, use information can also be stored within the sourceworks
21 extension, so that, for example, an owner of the server 94 or 104 can independently
22 track the use of his or her copyrighted works simply by downloading the
23 information at the server 94 or 104.

24

25 In general, each of the servers 94, 104 are owned and operated independently
26 from the other. By way of example, one typical owner of the server 94 is a
27 multimedia house which generates copyrighted works for sale and distribution.
28 Such an owner thus seeks to restrict access to the media to authorized users, thereby
29 protecting the copyright.

1
2 Each of the servers 94, 104 also provides selected use-base information about
3 the CONTAINERS registered and licensed through the servers. Specifically, the
4 selected use-base information provides a way to assess charges to the owners of the
5 servers for services rendered in connection with the servers 94, 104. The use-base
6 information is available by physically accessing the server 94, 104; but is more
7 conveniently obtained by phoning the server and downloading the information
8 directly. This information is not available for general users; but is typically available
9 only to the administrator who set up the servers 94, 104 in the first place. This
10 administrator can, for example, receives fees from the respective owners of the
11 servers 94, 104 as part of this arrangement.

12
13 For example, such an administrator would make revenue for several
14 transactions and sales shown in Figure 6, including: (A) registrations of
15 CONTAINERS on both registration servers 94, 104; (B) one licensing transaction for
16 auxiliary permissions for user 96; (C) two licensing transactions for auxiliary
17 permissions for user 110; (D) two PACKAGER modules resident at the computers of
18 Author 92 and Derivative Author 100; (E) two registration modules to configure the
19 servers 92, 104; and (F) one SDK module resident at author 112 (typically, the SDK
20 includes a SYSTEM EXTENSION, VIEWER and PACKAGER).

21
22 Those skilled in the art should appreciate that Figure 6 is illustrative only, and
23 that many other configurations of a computer network are possible within the scope
24 of the invention. For example, the network 90 can include a multitude of registration
25 and authorization servers; and any connected computer which has the SYSTEM
26 EXTENSION (and VIEWER, if needed) can access media on the network up to the
27 minimum permissions authorized by the minimum permissions data set within the
28 CONTAINER housing the respective media.

29
30 The sections below provide more detail about the invention, and include

1 descriptive and operational commentary of the SYSTEM EXTENSION, VIEWER,
2 sourceworks information, User Registration & Certification, the PACKAGER, SDKs,
3 registration servers, and authorization servers, among others.

4
5 VIEWERs and SYSTEM EXTENSIONs

6
7 In conjunction with the SYSTEM EXTENSION, the VIEWER allows viewing
8 and editing of graphic, image, video, audio, and textual objects that are packaged
9 into a CONTAINER in accord with the invention. Where objects are individually
10 packaged, viewing and editing will be done within the window of the source
11 application or designated viewer. Where objects are content elements within a
12 compound document, in-place viewing and editing will be common, with an
13 external window session being optional. Data objects - i.e., media - that are
14 packaged according to the invention can be dragged and dropped, for example,
15 between OLE 2.0-compliant applications such that all attribute information
16 contained in the CONTAINER remains intact during such an operation.

17
18 The SYSTEM EXTENSION is required for viewing and editing any
19 CONTAINER. The PACKAGER and TOOLBOX are complementary to the SYSTEM
20 EXTENSION and one is required to package media within a CONTAINER, e.g., the
21 CONTAINER 20 of Figure 1A. Typically the PACKAGER or TOOLBOX is required
22 to create derivative works from a CONTAINER; but only the SYSTEM EXTENSION
23 is required by developers when the minimum permissions of the source works do
24 not require clearance. This might be common for so-called "public domain" free use
25 of works.

26
27 The SYSTEM EXTENSION examines certain attribute information
28 encapsulated with the data object in compliance with the CONTAINER format.
29 Operations on the data object from within the VIEWER or editor are restricted based
30 on the minimum permissions encapsulated with the data object and any Auxiliary

1 Permissions subsequently obtained for the data object. By way of example, the
2 "Container Info" window of Figure 7 provides a local summary of the document,
3 including all available minimum and auxiliary permissions.
4

5 The SYSTEM EXTENSION also facilitates on-line licensing of CONTAINER-
6 packaged works. Based on registration information encapsulated with the data, i.e.,
7 the Container ID, the SYSTEM EXTENSION contacts the CONTAINER's
8 Registration Server and initiates an authorization transaction. After the user is
9 authenticated (typically utilizing the user's RSA digital signature, whereby the user's
10 key is stamped by a certification authority), the user uses a template-like interface to
11 request auxiliary permissions, such as shown in Figure 7a. If the permissions request
12 does not match the user's requirements, the request may be edited, such as shown in
13 Figure 7b. Based on the available Transaction Rules in the database for the user's
14 classification, licensing terms are presented to the user, such as shown in Figure 7c.
15 If the terms are accepted, a digital certificate is issued containing the auxiliary
16 permissions for that specific derivative use and encrypted to that specific user.
17

18 The License Request window, such as shown in Figure 7a, is the entry point
19 for licensing transactions. The Registration Server is identified and the set of
20 requested permissions is displayed. If the User recently attempted an unauthorized
21 operation, the permissions displayed are those required by that operation. The user
22 has the option to edit the request, such as shown in Figure 7b, to proceed with the
23 transaction, or to cancel out. When the user has submitted the Request, a License
24 Agreement, exemplified in Figure 7c, is returned to a display terminal of the
25 requesting user. This interface, such as shown in Figure 7c, allows the user to verify
26 the terms of the agreement and to agree to those terms.
27

28 The SYSTEM EXTENSION can be used to obtain extensive information about
29 the authorship, ownership, and licensing terms of a creative work prior to any
30 licensing transaction. This information may be a combination of data permanently

1 encapsulated with the object, including for example authorship and basic document
2 information, and information stored on the registration server, including for
3 example copyright ownership, licensing terms, royalty schedules, and other
4 augmented document Information. Figure 7d illustrates the typical information
5 which is available from the Registration Server and which can be displayed in a
6 Registry Info window.

7 8 Source Works Information

9
10 The SYSTEM EXTENSION can also be used to obtain source works
11 information for the media object. The Sources Works Display, for example and as
12 shown in Figure 7e, presents the electronic record of any work from which the
13 current work is derived, and the available information about each of those works.

14 15 User Registration & Certification

16
17 A user who wishes to engage in an on-line transaction with a REGISTRY
18 typically presents an RSA-based, network-standard digital signature signed by a
19 recognized Certification Authority. Accordingly, SYSTEM EXTENSIONS and
20 PACKAGERS can contain RSA-based standardized procedures for creating and
21 managing public/private key pairs, for engaging in certification transactions, and
22 for becoming registered users. The Certification Authorities require human
23 intervention when authenticating an individual's personal information. When valid
24 information is received, the individual's key is stamped with a unique code from the
25 Certification Authority which recognizes its authenticity. This certification is
26 apparent before anything is encrypted to that key, and is apparent when the key is
27 used to verify a digital signature (which can only have been signed by the individual
28 using the matching key).

1 PACKAGER

2
3 The PACKAGER is used by authors and publishers to encapsulate
4 authorship, ownership, minimum use permissions, and source works information
5 with a creative work and in a secure package. During this encapsulation, the original
6 binary file format of the creative work is preserved. An object created by the
7 PACKAGER can stand alone, or can be incorporated in a compound multimedia
8 CONTAINER. The PACKAGER is required for any editing sessions which involve
9 CONTAINER-packaged works and which demand clearance for derivative use.

10

11 During an editing session, the PACKAGER maintains a list of all
12 CONTAINER-packaged source works, their minimum permissions, and any
13 auxiliary permissions which have been granted to the current work in progress. The
14 Source Works Manager window, such as shown in Figure 7f, allows the developer to
15 easily see the status of permissions for each work, to obtain detailed authorship,
16 ownership, and licensing information from the source work's registration server, and
17 to selectively obtain auxiliary permissions as required for each source work.

18

19 For example, the user can command the display of all CONTAINER-
20 packaged source works from the Source Works Manager window of Figure 7f. For
21 each individual source work, the user may review the minimum permissions and, if
22 available, any auxiliary permissions which have been issued. If the user chooses to
23 obtain auxiliary permissions or to upgrade the current set displayed, a licensing
24 transaction is initiated with the source-work's registration server.

25

26 Alternately, the PACKAGER can prompt the user to upgrade the permissions.
27 This happen during the registration process in the following way: after preparing the
28 CONTAINER data for the derivative work, including the requisite minimum
29 permissions, the user executes a Check Clearance, wherein all accumulated
30 permissions are checked against the minimum permissions which the developer

1 intends to encapsulate with the derivative work. All sourceworks with permissions
2 that are insufficient will be listed in the Clearance Status window.

3
4 The Check Clearances function is also applied to the set of Transaction Rules
5 which the developer intends to load on the Registration Server. The basic principle is
6 that a derivative work may not grant more rights to the use of a source work than
7 what was available before the derivative work was created.

8
9 Some of the CONTAINER information which is encapsulated with the data
10 object by the PACKAGER is prepared from context automatically. Other information
11 can or should be manually entered or selected by the user through the a dialog
12 window such as the DocInfo Editor Window of Figure 7g, such as:

13
14 (1) Revision Number: The revision number identifies a version of the
15 document format which the PACKAGER complies with.

16
17 (2) Data Format and Creator Application: This provides the type of data
18 contained within the CONTAINER, and the application environment which
19 created the CONTAINER. Note, however, that these fields may have reduced
20 functionality when used, for example, with OpenDoc and OLE 2.0. In such a
21 case, the DocInfo Editor can display the information, but it does not need to
22 be contained as a separate DocInfo field if the Object CONTAINER can be
23 interrogated for it.

24
25 (3) Minimum Permissions: As described above, the minimum
26 permissions template provides a way for the user to generate the minimum
27 permissions that are encapsulated in the CONTAINER. One acceptable set of
28 permissions, such as shown in connection with the Minimum Permissions
29 Editor window of Figure 7h, includes:

- 1 • Opening / Viewing restricted
- 2 • Modifications restricted
- 3 • Drag & Drop restricted
- 4 • Printing restricted
- 5 • Format Changes restricted
- 6 • Saves restricted
- 7 • Registration of derivative works required
- 8 • Store Source Works Extensions on Registration Server
- 9 • Require Source Works Extensions
- 10 • Restrict Source Works Extensions
- 11

12 (4) Source Works Extensions: The identification of source works
13 extensions is managed by the Source Works Manager, described, in part, in
14 connection with Figure 7f. The author of the works can also track unregistered
15 or non-CONTAINER-packaged source works using the Source Works
16 Manager, which allows authorship and ownership information to be textually
17 entered into the Registration Server's database when the derivative work is
18 registered. When information or authorization is requested, only contact
19 information will be provided.

20
21 (5) Digital Signature: The Digital Signature provides authenticity and
22 integrity of all information contained in the CONTAINER. One secure way to
23 do this is to attach a RSA digital signature to the CONTAINER, which is
24 provided by the registration server upon license. The author is a registered
25 user in this case, and the CONTAINER is registered on a Registration Server.
26 Appropriate evidence of certification and the CONTAINER's hash results are
27 contained in the signature.

28
29 The PACKAGER can also enable encryption of the media within a
30 CONTAINER. If an author chooses to encrypt the media, a random key for the
31 media is generated; and during a secure registration transaction with the registration
32 server - such as after a log-on and once the author proves she is authorized to use the
33 server - the secret key is passed by either (i) a secure communication channel, or (ii)

1 a certificate that is public-key encrypted to the user's key, so that only that user may
2 use that issuance of the secret key. This encryption method provides for strong
3 security since secret keys are randomly generated and are unique to a CONTAINER;
4 and the distribution of the key to the CONTAINER is handled by the server.

5
6 Those skilled in the art will appreciate that other encryption methods are
7 suitable for use with the invention and without departing from the scope of the
8 invention.

9
10
11 SDKs

12
13 As discussed above, the Software Development Kit (the SDK) enables
14 developers of advanced multimedia applications, games, or multimedia authoring
15 tools (including content creation applications) to incorporate SYSTEM EXTENSION,
16 VIEWER and PACKAGER functionality into their applications in advanced ways.
17 The SDK is appropriate, for example, when conventional OLE 2.0 compliance does
18 not deliver the functionality or performance that the ISV demands.

19
20 The SYSTEM EXTENSIONs, VIEWERs and PACKAGERs of the invention
21 operate with most OLE 2.0-compliant content creation tools and with most tools that
22 create compound works. The SDK permits the developers to follow their own
23 coding standards but still take advantage of the invention.

24
25 Registration Server

26
27 The Registration Server of the invention contains the set of services used by
28 information creators who want users of their works to be able to easily identify
29 ownership, obtain licensing terms, and license those works on-line. The
30 Authorization Server module is the set of services those information users (who may
31 also be information creators) will use to obtain access to information and license

1 those works. The Server maintains a database of registry information pertaining to
2 creative works which rights-holders are making available for commerce.

3
4 The process of initiating a database entry for a work is called Registration.
5 The act of processing a user's request for augmented permissions is called
6 Authorization or licensing. Before starting a transaction with the Server, the
7 PACKAGER does the following:

- 8
9 • Verify that the user is a registered user. It will look for the user's RSA key
10 with a certification stamp from an approved certification authority.
11 Preferably, user registration capabilities are built into all VIEWERs and
12 PACKAGERs.
13
- 14 • Ensure that the user completes the Transaction Rule Templates, used in
15 designing the licensing rules for all available classes of users. This should
16 be completed prior to contacting the Server because they determine
17 whether sufficient clearances have been obtained.
18
- 19 • Ensures that the user completes the Ownership Information Template,
20 which is the textual information that a user of the work would receive
21 when using the VIEWER to obtain further ownership information, beyond
22 what might be encapsulated in that package.
23
- 24 • Verifies that sufficient clearances (auxiliary permissions) for all source
25 works used in the current work-in-progress are available to the
26 PACKAGER.
27
- 28 • If the clearances are insufficient, the PACKAGER guides the user through
29 the series of authorization transactions required to get the necessary
30 permissions.

- When sourceworks clearances are complete, the PACKAGER performs a one-way hash function contained, for example, in an RSA Digital Signature and which become part of the works' database record for later authentication.

- As a last step, the PACKAGER contacts the Server.

The PACKAGER testifies to the Server that the user is authentic and that all sourceworks (if any) used in the work being registered have been properly cleared. The Server then assigns a unique registration ID to the CONTAINER (based, for example, on the server's ID and the number of documents registered on the server) and builds the database record based on the information held by the PACKAGER.

In "signing" the CONTAINER, the PACKAGER preferably assembles a RSA Digital Signature for the package. Contained within the signature are the registration ID and the results of the one-way hash on the document data. The signature is encrypted to the User's key, thus demonstrating authenticity.

Authorization Server Module

Before starting a licensing transaction with the Authorization Server, the SYSTEM EXTENSION does the following:

- Determines that available permissions (minimum and auxiliary) are not sufficient to perform the user's desired action.
- Verifies that the user is a registered, which is required only if a transaction with the Server is necessary.
- Testifies that the user is registered and presents the authorization request (a request for specific auxiliary permissions) to the Authorization Server.

1 The user's classification is also transferred and stamped with certification
2 from the associated Certification Authority.

3
4 Based on the requested auxiliary permissions and the classification of the
5 user, the Server presents its terms for licensing. These terms are viewable within a
6 display window and can include, without limitation, any of:

- 7
- 8 • Actual permissions granted
 - 9 • Payment options. When a choice of on-line payment methods are
10 available, a provider-specific window becomes available after the method
11 is chosen. When some other method is required, an appropriate window
12 to facilitate the payment is displayed.
 - 13 • Request human intervention. The user or the Server may not be satisfied
14 with an on-line authorization request. In that case, the option exists to
15 pursue some form of human intervention. The options which the
16 registering party has made available are displayed.
 - 17 • Accept terms. When the licensing terms are accepted, a packet
18 enabling the auxiliary permissions is transferred to the user's computer.
19 These are encrypted to the user and thus are non-transferable.
- 20

21 The systems and methods of the invention encompass novel methods and
22 tools which will enable creators of networked multimedia programs to identify their
23 media and to claim their rights. This is enabled, in part, by bundling the copyright
24 information with the data element, and by formatting the CONTAINER in a manner
25 which maintains this identification and attribution so that it persists with the
26 copyrighted work through generations of derivative use. The invention therefore
27 demonstrates the application of copyright permissions to a hierarchy of network-
28 distributed data objects to effectively protect owners' rights.

29

1 This invention also facilitates the licensing of multimedia content by different
2 classes of users. In accord with the invention, a desktop tool can be integrated with
3 selected viewing or production tools to feature an interactive licensing template. The
4 invention thus demonstrates the integrated support of hierarchical permissions
5 headers in the production environment, and demonstrates networked interactive
6 licensing within the production environment based on hierarchical permissions.

7
8 Figure 8 illustrates one acceptable process flow for managing copyrighted
9 works in accord with the invention and corresponding to the methods and systems
10 described herein.

11
12 Figure 9 illustrates a system 200 constructed according to the invention. The
13 system 200 includes a server 202 which operates as a registration and authorization
14 server for any of the CONTAINERS 204a, 204b, 204c, and 204d stored in a library
15 206. By way of example, the library 206 can be a publisher's library of any or all of
16 the original works owned by or authored for the publisher. Author 208, for example,
17 illustrates one such author connected to the library 206 through a personal computer
18 210 and communication line 212. The computer 210 is a data processor that includes
19 a PACKAGER 214 constructed according to the invention and as described
20 hereinabove. In the preferred embodiment, the PACKAGER 214 is a software
21 module stored within the computer's internal memory 210a to control the data
22 processor's actions in accord with the invention. Through the PACKAGER 214, the
23 author 208 can create and package any of the CONTAINERS 204. The computer 210
24 also includes a communication section 210b, to facilitate on-line communications,
25 and a computer display 210c.

26
27 The CONTAINERS 204 are secure containers of electronic media, as described
28 herein, and are stored in the library 206 as digital files, such as within a CD-ROM, or
29 within a computer memory. Preferably, the CONTAINERS are stored such that a

1 user such as User 216 can access the CONTAINERS through an on-line connection
2 218 between the user's personal computer 220 and the library 206.

3
4 The owner of the library 206 may also have copyrights in CONTAINERS such
5 as CONTAINER 204e, which represents a CD-ROM of a media-packaged work that
6 is distributed to the User 216 by mail. The CD-ROM 204e, for example, exemplifies
7 one other published work that is created by the author 208 and packaged by the
8 PACKAGER 214. As above, the server 202 also functions as the registration and
9 authorization server for CONTAINER 204e.

10
11 In accord with the invention, the user's computer 220 is a data processor that
12 includes a SYSTEM EXTENSION 222 constructed according to the invention and as
13 described hereinabove. In the preferred embodiment, the SYSTEM EXTENSION 222
14 is a software module stored within the computer's internal memory 220a to control
15 the data processor's actions in accord with the invention. A CD-ROM 224 drive is
16 preferably connected to the user's computer 220 via data line 220d to facilitate access
17 to CD-ROM files such as CONTAINER 204e.

18
19 Through the SYSTEM EXTENSION 222 (and a VIEWER, if needed), User 216
20 can access any of the CONTAINERS 204a-e up to the minimum permissions
21 authorized by each of the CONTAINERS. By way of example, the minimum
22 permissions data set within each CONTAINER typically authorizes the User 216 to
23 view the CONTAINERS 204a-e; but not to download, modify, save or otherwise
24 electronically transfer the CONTAINERS. The data transfers required to access the
25 CONTAINERS 204a-d up to the minimum permissions data set occur through
26 communication line 218; while the only data transfers required to access the
27 CONTAINER 204e up to its minimum permissions data set are between the
28 computer 220 and the CD-ROM drive 224.

29

1 If the User 216 wishes to augment the authorizations to any of the
2 CONTAINERS 204, for example to modify or save the CONTAINER at the computer
3 220, she must communicate with the server 202 and transact a license with that
4 server. The data processor 220 thus includes a communication section 220b that is
5 connected for data transfers, over communication line 226, with a compatible
6 communication section 202a of the server 202. Upon selection by the User 216, the
7 VIEWER 222 determines from the selected CONTAINER 204 that authorization
8 server 202 is assigned to handle all licenses to that CONTAINER, and the SYSTEM
9 EXTENSION controls the computer 220 to connect to the server 202 at the right
10 address so that an on-line licensing transaction can occur.

11

12 Specifically, once the user 216 indicates that additional permissions to the
13 CONTAINER 204 are desired, the SYSTEM EXTENSION can display selected terms
14 to the CONTAINER, as stored within the CONTAINER or as stored within the
15 server 202. In either case, the SYSTEM EXTENSION causes the computer 220 to
16 generate a licensing request signal and issue that signal to the server 202. Preferably,
17 the user 216 also designates - through the SYSTEM EXTENSION - the desired use of
18 the media within the CONTAINER. The user 216 can thereafter accept the licensing
19 terms to the CONTAINER 204, and, if accepted, the user 216 receives notification
20 from the server 202 that auxiliary permissions are granted for the desired use.

21

22 In the event that CONTAINER 204 is a derivative work, the SYSTEM
23 EXTENSION 222 determines that auxiliary permissions are also required, for
24 example, from server 228, the server designated by the original author of the media
25 within CONTAINER 204.

26

27 The server 202 stores transactional information about the CONTAINERS 204.
28 For example, each license transacted through the server 202 is stored in a file 229a,
29 such as within a computer memory 230. In this way, the owner or administrator of
30 the CONTAINERS can assess the licensing fees generated by the CONTAINERS.

1 Likewise, the server 202 also stores information or files 229b that set forth the
2 number of CONTAINERS registered thereon, so that, again, the owner or
3 CONTAINER-administrator can assess server usage. The files 229a, 229b are
4 preferably available through the communication section 202a.

5
6 In one embodiment of the invention, the server 202 includes an internal
7 memory 202b, connected to the communication section 202a, that stores selected
8 information about the CONTAINERS registered thereon. For example, licensing
9 terms to the CONTAINER 204 can be stored within the memory 202b. A relay
10 section 202c operates to relay such terms to the processor 220 in response to a license
11 request signal prompted by the user 216. A data comparison section 220d operates to
12 compare the user's reply to the licensing terms, and to generate and transmit the
13 requested auxiliary permissions when the response signals correspond to the
14 requisite terms specified in the license information stored in memory 202b (or
15 alternatively in the CONTAINER). Accordingly, once the user 216 receives the
16 auxiliary permissions, that user is provided with additional authorizations to use the
17 media within the CONTAINER 204; and the SYSTEM EXTENSION 222 enables the
18 user 216 to access the CONTAINER 204 up to the maximums allowed in the
19 bumped-up permissions data set.

20
21 Figure 10 illustrates a system 298, constructed according to the invention, and
22 provides a brief description of several components of the invention; and further
23 illustrates certain relationships between such components. First, the system 298
24 provides for the making and manipulation of CONTAINERS 300 and 301. As
25 illustrated, a CONTAINER such as CONTAINER 300 can occupy a single block of
26 memory such within memory 302 (e.g., memory 302 can be solid state RAM within
27 a computer 304, or ROM memory within a web server 304). Each CONTAINER has
28 one or more Digital Creative Works and Metadata. The CONTAINER 300, for
29 example, has DIGITAL CREATIVE WORK 306 and associated METADATA 308.
30 The WORK 306 is the electronic expression created, for example, by an author or

1 publisher, and is shown as a letter "Z" for clarity of illustration. The METADATA
2 308 provides selected information about the WORK 306; and such information can
3 include, for example, the author's name, the minimum permissions or minimum
4 authorized uses of the WORK 306, and licensing details.

5
6 A CONTAINER can also occupy a plurality of locations on the Internet 307.
7 This is illustrated by CONTAINER 301, which has several parts 301a, 301b and 301c
8 linked through the Internet 307. As illustrated, for example, the CONTAINER 301
9 includes DIGITAL CREATIVE WORK 310a and 310b, each at a different location
10 312a, 312b, respectively; and METADATA 314b and 314c, each at a different location
11 312b and 312c, respectively. For illustrative purposes, location 312c is here shown as
12 a REGISTRY 316 that serves as the registration server for CONTAINER 301.

13
14 The computer 318 illustrates one of a number of users of the Internet 307. As
15 such, computer 318 typically houses web browser software 320, such as Internet
16 Explorer™, within internal memory 322. The computer 318 also has communication
17 software and hardware 326 which facilitates communication with the Internet 307.

18
19 Other software is also present within the computer 318. Within the operating
20 system memory 328, there resides a SYSTEM EXTENSION 330 which recognizes
21 and which enables interaction with CONTAINERS such as CONTAINERS 300, 301.
22 By way of example, a user at computer 318 can surf the WWW (i.e., the Internet 307)
23 and locate the CONTAINER 301 at web server 304. The CONTAINER 301 can be, for
24 example, displayed on a web page at the user's screen 332 as OBJECT "Z" that
25 instantiates the CONTAINER 301. In the event the computer 318 does not have the
26 EXTENSION 330 installed thereon, the CONTAINER 301 can include, within the
27 METADATA 308, a location on the WWW 307 to find and obtain such a SYSTEM
28 EXTENSION 330. One location, for example, can be an administrative web site 334
29 that is also connected to the WWW 307 with a unique web address. When
30 requested, the site 334 downloads the EXTENSION 330 to the computer 318 so that

1 the computer 318 can render the OBJECT "Z". Since the OBJECT "Z" is generally a
2 graphic or text, e.g., a JPEG or Microsoft Word™ document, that was formed by a
3 third party application software, then the computer 318 should further house, for
4 example, a "VIEWER" 336 such as a JPEG viewer or the Microsoft Word™
5 application.

6
7 In operation, a user thus sees the OBJECT "Z" which instantiates the
8 CONTAINER 300. Normally, the user at computer 318 will not notice anything
9 different about the OBJECT "Z" as compared to any other graphic or visual within a
10 web page. However, when the user clicks on the OBJECT "Z" by operation of the
11 mouse 318a, then that user will be given additional information, such as the
12 associated METADATA 308. Further, if the user at computer 318 attempts an
13 operation - e.g., copying into another file or printing on the printer 318b - that is
14 prohibited according to the instructions in the METADATA 308, then that user will
15 be so notified and informed that a license is needed to accomplish that action.

16
17 By way of example, suppose the CONTAINER 300 is registered at the
18 REGISTRY 338, which is a registration server for the CONTAINER 300. When the
19 user at computer 318 is notified of an improper operation, the user will be given the
20 opportunity to obtain a license to the Digital Creative Work 306 through interaction
21 with the REGISTRY 338. The METADATA 308 specifies that registration server 338
22 is designated with this role; and further specifies the REGISTRY address so that the
23 computer 318 can locate the REGISTRY 338 on the WWW 307.

24
25 Figure 10 also illustrates a second computer 340 that represents an author or
26 publisher of Digital Creative Works. As such, the invention provides a way to
27 package the Work with a CONTAINER. For example, computer 340 includes a
28 PACKAGER or TOOLBOX 342 which packages Digital Creative Work such as the
29 work 344 on the screen 340c, here illustrated as the letter "Y". Typically, the Work
30 344 is made by a third party application, e.g., Adobe Photoshop™. As such, the

1 computer 340 typically includes this software within internal memory. In Figure 10,
2 this software is referred to as VIEWER 346 because the application is typically the
3 same application that is later required to view or utilize the Work 344.

4
5 Once the user at computer 340 packages the Work 344 within a CONTAINER
6 348, the Work 344 will have attribution for any location on the web 307. As such, the
7 user at computer 340 can send the CONTAINER 348 onto the Internet 307 for
8 storage, if desired, at a web site or at a REGISTRY such as REGISTRY 338. When
9 other users, e.g., a user at computer 318 locate and access the CONTAINER 348,
10 such a user sees the OBJECT "Y" as the instantiation of the CONTAINER 348. If the
11 user attempts an operation that is prohibited, then the CONTAINER 348, through its
12 Metadata, locates and phones its home, which in this example is the REGISTRY 338,
13 to begin a licensing transaction.

14
15 Figure 11 illustrates a system 400 constructed according to the invention.
16 Figure 400 further illustrates general and preferred operations and functionality of
17 the system 400 in the management of Digital Creative Works. In Figure 11, user
18 stations 402 and 404 are computers for users of digital media connected to the
19 Internet 406 and to each other via a network or Intranet 408. User stations 402 and
20 404 are connected to the Internet, and to the Intranet 408, via local data lines 402b
21 and 404b, respectively.

22
23 User stations 410 and 412 are used by creators or authors of Digital Creative
24 Works 410a, 412a, respectively; and are connected to the Internet 406 by data lines
25 410b and 412b, respectively. Digital Creative Work 410a is shown illustratively as an
26 "A" on the screen 410c of user station 410; while Digital Creative Work 412a is
27 illustratively shown as an "A+B" on screen 412c of user station 412. The Work 412a
28 is denoted as "A+B" to indicate that the Work 412a is a combination of creative
29 works of both authors at stations 410 and 412.

1
2 Those skilled in the art should appreciate that each of the stations 402, 404,
3 410 and 412 have hardware (not shown) which enables communication with the
4 Internet 408 and/or Intranet 406. For example, such hardware often includes a
5 modem and supporting software to facilitate communication through the Internet
6 408, to other users, such as through email, and to selected web sites, FTP sites, URLs,
7 newsgroups, databases, and the like.

8
9 User station 410 also has a TOOLBOX 414; and user station 412 has a
10 PACKAGER 416. The TOOLBOX 414 and/or PACKAGER 416 are used to create a
11 CONTAINERS, here illustrated as CONTAINERS 418 and 420. CONTAINER 418
12 derives from the work 410a of station 410; while CONTAINER 420 derives from the
13 work 410a and the work 412a of station 412. CONTAINERS 418 and 420 are shown
14 connected to the data lines 410b, 412b to illustrate that the CONTAINERS are
15 transmitted through, or dispersed on, the Internet 408.

16
17 Each of the user stations 402, 404, 410 and 412 has a SYSTEM EXTENSION
18 422 installed into an associated internal memory 402d, 404d, 410d and 412d,
19 respectively. These EXTENSIONS 422 operate with the operating system of the
20 associated station so as to recognize, interact with, and access CONTAINERS.

21
22 User stations 402 and 404 additionally have VIEWERS 424 installed into
23 internal memory 402d and 404d, respectively. The VIEWERS 424 are used to view
24 and interact with the Works within CONTAINERS. By way of example, if an
25 OBJECT 410a is a graphic that is best viewed with a JPEG VIEWER, then the
26 EXTENSION 422 calls that VIEWER to render the OBJECT 410a as needed to the
27 user 402. Note that user 402 sees the OBJECT "A" as the instantiation of the
28 CONTAINER 410. Likewise, user 404 sees the OBJECT "A+B" as the instantiation of
29 the CONTAINER 420.

1
2 The Registry 426 operates to register selected CONTAINERS, and to negotiate
3 as agent for any author of a CONTAINER. Preferably, the Registry 426 has internal
4 memory 426d which can be used to store CONTAINERS, METADATA to
5 CONTAINERS, or parts of CONTAINERS and/or METADATA. It is important to
6 note that a CONTAINER need not reside at a single memory location. Those skilled
7 in the art will appreciate that a CONTAINER based on object technology can be, and
8 is intended to be, dispersed across the Internet 408 so that different portions of the
9 CONTAINER reside at the most logical location for that portion.

10
11 For illustration purposes, Figure 11 also shows an administrative site 428 (and
12 associated Registry 428a), which can operate to augment the system 400, as
13 described below; and a generic web site 430 that provides database information such
14 as commonly provided on the WWW. As above, those skilled in the art should
15 appreciate that the administration site 428 and web site 430 include associated
16 hardware (not shown) to facilitate the needed communication with the Internet 408
17 and other users 402, 404, 410 and 412 of data therein.

18
19 In operation, the system 400 has many features, some of which are illustrated
20 in Figure 10. Specifically, work 410a is instantiated on the screen 410a as OBJECT
21 "A." By way of example, "A" can represent a digital representation of a drawing or
22 sketch by the author. By way of further examples, "A" can be made electronically,
23 such as through a graphic artist program (using the keyboard 410f and mouse 410g)
24 such as Adobe Illustrator™; or "A" can be hand-drawn and scanned within the
25 computer 410 by an optical scanner, such as known to those skilled in the art.

26
27 In one example, the author of CONTAINER 418 makes the Digital Work "A"
28 for enjoyment only; and does not choose to register the CONTAINER 418 with the
29 REGISTRY 426. However, the author at station 410 does desire recognition as the
30 author of the work "A," so he encapsulates METADATA 418b within the

1 CONTAINER 418 that specifies his name. User 410 thereafter sends the
2 CONTAINER 418 onto the Internet 406, where it is stored as a web page at the
3 database or web-site 430.

4

5 Other users, connected to the Internet 408 and web-site 430, who have a
6 SYSTEM EXTENSION resident at their computer, can access the OBJECT "A" of
7 CONTAINER 418. By clicking on the OBJECT A, or through such other authorized
8 action as specified by the author 410, such a user can additionally obtain information
9 about the author's name in the METADATA 418a.

10

11 By way of example, the user at user station 402 is interrogating the Internet
12 408 through visual interaction with her display 402c of the WWW (note for clarity of
13 illustration that no accompanying mouse and keyboard are illustrated with user
14 stations 402 and 404; and even though they are not required, it is intended that such
15 instruments are present). User 402 accordingly has web browser software 432 (e.g.,
16 Netscape™ and Microsoft Internet Explorer™) installed in internal memory 402d on
17 the computer 402. When the user at station 402 encounters the web page with the
18 CONTAINER 418, typically seen as OBJECT A referring to the CONTAINER 418, the
19 SYSTEM EXTENSION 422 and VIEWER 424 permit viewing of the OBJECT "A." The
20 author's name can also be displayed, if desired, through the METADATA and as
21 specified by the author at station 410.

22

23 Note, again, that because the CONTAINER 418 is integrated with object
24 controls utilizing ActiveX™, or similar object control, the CONTAINER 418 need not
25 comprise data that is resident at the same location. Rather, a CONTAINER can
26 include data that is spread across the network 406 or Internet 408. Because the
27 CONTAINER 418 is formed with object-based controls, when user station 402
28 encounters the web page at site 430 that refers to the CONTAINER 418, the
29 computer 402 first interrogates its registry to see if that control is available internally.

1 If not, the computer automatically finds and installs the control over the Internet 408
2 based upon the address specified by the author at station 410.

3
4 The user at station 412 represents an author and a user of CONTAINERs. In
5 particular, user station 412 has a SYSTEM EXTENSION 422 within internal memory
6 412d so that it can access the CONTAINER 418 at web site 430. In this example, the
7 user at station 412 chooses to edit the CONTAINER 418 through use of the
8 PACKAGER 416, also resident in memory 412d, so that the CONTAINER 420
9 contains both digital creative works 412a and METADATA as selected by the user at
10 station 412. The work 412a is illustratively shown as "A+B" in Figure 1.

11
12 Accordingly, the work 412a created at station 412 is "derivative" in nature,
13 since it derives from previous artistic work (i.e., the work 410a) of the author at
14 station 410. The invention keeps track of the derivative uses and edits of digital
15 creative works in a source works file disposed within the METADATA, as described
16 herein.

17
18 In this example, the user at station 412 chooses to register the work 412a with
19 the Registry 426. Accordingly, the user at station 412 first initiates a registration
20 request to communicate and request registration of CONTAINER 420. Depending on
21 the type of work 412a, the user at station 412 can select a corresponding property
22 page template to identify and select certain METADATA as associated with the
23 CONTAINER 420. By way of example, any of the following information can be - or
24 are required to be - communicated to the Registry 426, depending upon how the
25 particular Registry is set up:

- 26
27 • The author's name and other rights related information (attributes or
28 properties) of the work 412a.
29 • The aesthetic presentation of the attached information (METADATA)
30 for the work 412a.

- 1 • The balance between accessibility and locality of the CONTAINER's
2 properties. For example, certain static METADATA, such as the author's
3 name, can be located in the CONTAINER 420; whereas requests for volatile
4 METADATA information, such as quantity of works 412a to be published, is
5 generally referred to a remote server. For example, the web site 430 or station
6 412 can each function as such a remote server; and the author at station 412
7 can specify, or change, the number of published quantities of the work 412a as
8 needed.
- 9 • The minimum permissions, auxiliary permissions and requirements for
10 use of the work 412a by any user.
- 11 • The specification of other services, such as email, that are available
12 through access to the CONTAINER 420.
- 13 • The sets of attributes, presentations, and permissions that are applied
14 to the multiple works 410a and 412a.
- 15 • The specification of prototypes or templates of sets of attributes,
16 presentations, and permissions that are formally and legally appropriate to
17 the works 410a and 412a.
- 18 • The organization of attribution and credit to the work 410a, since the
19 work 412a is a derivative work.
- 20 • The REGISTRY can have multiple templates available for different
21 business models, different media types, and different categories of registrants.
- 22 • The subsequent processing by Registry 426 in evaluating, granting, and
23 tracking permitted uses of the work 412a.
- 24 • Structure to comply with the protocols established by various
25 registries. Note that although a single Registry 426 is illustrated in Figure 1,
26 multiple registries are possible and intended. For example, had the user at
27 station 410 registered the work 410a at a Registry other than Registry 426,
28 then that Registry would require certain protocols and information (e.g.,
29 addresses) to identify that Registry and to communicate thereto.

1
2 This example is not a common occurrence whereby the original creator, user
3 410, chose to make an unregistered OBJECT "A". Such a creator 410 thus preferably
4 makes the unregistered OBJECT A with "open" permissions so that the associated
5 Work 410a can be incorporated into other works, e.g., the Work 412a. Once the
6 derivative user 412 uses the Work 410a, then the identification of the original author,
7 i.e., "source work", will be reflected in the source works page of the new template, if
8 available. The onus is on the user to contact the creator by whatever means that
9 creator lists in the property pages of the unregistered OBJECT A, possibly a phone,
10 fax, email, or other contact. As such, an unregistered OBJECT can carry substantially
11 all the information of a registered object.

12
13 The users at stations 410 and 412 can thus package CONTAINERS from
14 within creativity tools, within an Application Programming Interface (API) for a
15 particular plug-in, or directly from the shell: in the case of the user at station 410, the
16 TOOLBOX 414 indicates that the work 410a was created from within a creativity tool
17 such as Adobe Illustrator™; while station 412 has a PACKAGER 416 installed as a
18 direct shell application to produce CONTAINERS. These tools, together with the
19 registration process at the Registry 426, assure the user that the attached
20 METADATA information is not easily removed, altered or forged. Such users are
21 then able to catalog, share, and generally manipulate such sets in an organized way;
22 and with a large degree of automated help from the system 400. The attached
23 METADATA information is accessible from any representation of the works 410a
24 and 412a, especially from a rendition of the content as well as any iconic ones.

25
26 User station 404 is very similar to the user station 402, except that the user at
27 station 404 has accessed a registered work 412a, as opposed to the unregistered work
28 410a in CONTAINER 418. Accordingly, the METADATA 420b of CONTAINER 420
29 specifies the minimum permissions of the work 412a. Typically, for example, that
30 minimum permissions allows the user 404 to view the work 412a on the screen 404c;

1 yet further actions such as print, copy, drag and drop are prohibited and are not
2 possible without a license to the work 412a. By way of example, if the user at user
3 station 404 desires to print fifty copies of the work 412a, then a license to this activity
4 must be negotiated through the Registry 426, where the CONTAINER 420 was
5 registered. If the METADATA 420b permits the license of the work 412a in terms of
6 the number of prints, then the user at station 404 can contact the Registry 426 and
7 proceed with appropriate licensing terms.

8
9 Once created, CONTAINERS live on as data items within the Internet 408. It is
10 likely that the individual or company which created the work associated with a
11 particular work no longer exists relative to the Internet 408 and Registry 426. For
12 example, one creator of Digital Creative Works is a publisher of magazines; and if
13 that magazine goes out of business, then subsequent licenses to their works are
14 problematic. There are several ways to deal with this problem. First, the publisher in
15 such a situation can notify the Registry that it is going out of business and that future
16 transactions as to their CONTAINERS are prohibited. Alternatively, the publisher
17 can inform change the METADATA within the CONTAINER so as to unregister the
18 CONTAINER, thereby providing a free license to the works within the
19 CONTAINER. Note that the publisher could specify, in the METADATA,
20 information about the publisher and suggestions for alternative contact points; and
21 that METADATA is available to users with VIEWERS.

22
23 In a default situation, where the publisher does nothing relative to its
24 orphaned CONTAINERS, the Registry 426 can contact the administrative site 428 to
25 decide the fate of the CONTAINER. At that point, the administrative site can specify
26 that no additional information is known; and, for example, that access to the
27 CONTAINER is prohibited.

28
29 The administration site 428 also operates in default situations where the
30 Registry does not answer. In that case, the administration site 428 can review the

1 status of the CONTAINER and inform the requesting user to call the Registry later,
2 for example if a temporary problem exists or if the Registry is too busy.
3 Alternatively, the administrative site can function as an alternative Registry, if set up
4 by the creator of the CONTAINER.

5
6 The invention thus supports commerce between the owners and creators of
7 digital content, i.e., the Digital Creative Work. Specifically, the invention provides a
8 method for the owner to license the work, while also providing a method for the
9 multimedia developers and publishers to make productive use of the work's
10 content. The invention thus provides a uniform, timely, and persistent means of
11 identifying digital content in the networked environment.

12
13 In a preferred embodiment of the invention, an Internet-based application is
14 built around the OBJECT as supported by the TOOLBOX and the Registration
15 Server. The SYSTEM EXTENSION enables OBJECTS to be viewed on target
16 operating systems and from within a variety of applications. Preferably, the
17 invention incorporates object technology such as Internet-extended OLE, the
18 standard object technology developed by Microsoft™ that allows a variety of media
19 types to be shared by applications throughout the Internet. One such interaction,
20 according to the invention, is illustrated in Figure 12.

21
22 The invention also provides substantially uniform representation of content
23 within other applications. That is, creativity tools such as graphics, sound, video,
24 word processing, and multimedia authoring tools are presented with a substantially
25 uniform interface to host applications, relieving those applications from the
26 responsibility of rendering all media types. Further, the creators and owners of
27 content (i.e., Digital Creative Works) can, with the invention, store and make
28 available the METADATA which can be critical to licensing and other derivative
29 uses.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

The invention creates documents, or CONTAINERS, through a process called packaging. The PACKAGER merges content (i.e., Digital Creative Work), Metadata, and active interface controls and presents this to the user through a set of property pages designed for the specific business problem being addressed. The result of this packaging is instantiated as an OBJECT. Figure 13 illustrates one packaging process according to the invention. In Figure 13, Digital Creative Work and Metadata associated with that content are combined with the desired template to create the OBJECT.

For an owner or creator, a CONTAINER is much easier to track and to manage than conventional content because the Metadata is accessible directly from the CONTAINER. Typically, the owner or creator will choose to attach a small amount of identifying data to the Digital Creative Work, with the larger and/or most volatile data being supplied to the CONTAINER from a remote registration server via the Internet. After the work is packaged as a CONTAINER, owners and creators can ensure that potential users always obtain up-to-date ownership, contact, and licensing information about specific content elements. Owners can thus be sure that the positive identification, direct communications, and possibility of automated licensing will maximize the likelihood that their content will get used in legitimate or legal derivative works.

CONTAINERS also reduce the workload of multimedia developers, publishers, and other derivative users of content by making the identification of content and its ownership substantially instantaneous and by reducing or eliminating delays, errors and misdirection when communicating with the appropriate rights management authorities.

In accord with the invention, one way to convert Digital Creative Works to CONTAINERS and OBJECTs begins with the use of a Template Editor. The

1 Template Editor presents an interface for designing sets of properties and property
2 pages that organize the presentation of the CONTAINER's Metadata and buttons
3 that initiate various functions of the OBJECT. Specifically, the Template Editor
4 enables content owners to create layouts for property pages, placing various controls
5 on the pages. These controls can, without limitation, include:

- 6
- 7 • Fields for static data that will ultimately be bound to the object
- 8 • Fields for dynamic data that will ultimately be stored on a remote server
- 9 • Labels for clarifying or identifying sections of the property page
- 10 • Buttons for initiating an email or web access action
- 11 • Buttons for retrieving dynamic data from a remote server
- 12 • Other elements including illustrations, logos, or icons
- 13

14 One illustrative property page template is shown in Figure 14. Another template
15 and an associated OBJECT, instantiating a CONTAINER, is shown, representatively,
16 in Figure 15.

17

18 After creating the property page template, a user of the invention can employ
19 one of several tools to make the CONTAINER: the Toolbox, the Express Packager,
20 and the Software Developers Kit (SDK). Each tool merges the various input elements
21 to create a CONTAINER or Object. In one illustrative case, the user of the tool
22 specifies the source content element (e.g., photo, sound, video, text, etc.) and the
23 Template to be used in the packaging process. The user then supplies the data
24 required by the Template. Once all the data is supplied, the PACKAGER, taking its
25 basic instructions from the Template, creates the CONTAINER, binding static data
26 to the content and automatically storing dynamic data on the designated
27 Registration Server. The various PACKAGER tools are designed for different
28 applications and needs:

- 29 • In one configuration, the TOOLBOX is a graphical desktop tool designed for
30 individual users packaging relatively small amounts of content. From a standard
31 graphical user interface, the user specifies the content source file and designates
32 the appropriate Template. The Toolbox then prompts the user for the necessary

1 input to complete the required entries specified by the Template. Upon
2 completion of the required entries, the Toolbox will update the associated server
3 with dynamic data, if any, and create a CONTAINER.

4 • The Express Packager is a batch-oriented PACKAGER tool which converts
5 high volume content elements to CONTAINERS. When using the Express
6 Packager, the operator specifies a set of content files, the template, and a source
7 of the required input data. The Express Packager then automatically accepts the
8 input and converts the files to the right format.

9 • The SDK Packager is designed for applications where functionality according
10 to the invention is to be built into existing content production tools. As an
11 example, certain Internet publishers provide various "just-in-time" content
12 delivery systems. In such a case, the SDK Packager is used whereby the
13 publisher's existing production tools automatically invoke the packaging process
14 to follow the same model of receiving content, template, and data as input to
15 produce the CONTAINER.

16
17 In the process of packaging, an owner can create a registered object by
18 communicating with the Registration Server. Alternatively, the owner can use one of
19 the packaging tools to create an unregistered object. In such a case, static information
20 is bound to the content but there is no record placed on a Registration Server.

21
22 The Registration Server provides the communications link to Objects. Usually,
23 it is the creator of the Template who establishes the relationships between the
24 dynamic data required by the Object and the Registration Server. The Registration
25 Server listens for various types of requests entered by viewers of the content (i.e., the
26 Digital Creative Work). Those requests can be for specific elements of data that will
27 be displayed on property pages, or for other data that will support functions such as
28 email or web site addressing. The requests may also include transactions that require
29 interfacing to legacy business systems or financial transaction systems.

1
2 The Registration Server is built to respond to such requests and to interface
3 with existing information and transaction systems. In such a role, it can:

- 4
- 5 • Retrieve product information or pricing from a vendor's remote database and
6 supply it so it can be displayed on a property page.
 - 7 • Retrieve content ownership, contact, and licensing information from a
8 publisher's remote database.
 - 9 • Receive an incoming payment request and submit it to a third-party payment
10 handling system.
 - 11 • Supply transaction activity data to an in-house marketing database.
- 12

13 Many institutional content owners with existing business information and
14 transaction systems can choose to have those systems interoperate with, or as, the
15 Registration Server. Other users, however, can opt for an Administration Server.
16 The Administration Server is a database that contains document and business
17 information and transaction rules pertaining to owner's distributed content. The
18 Administration Server is used to supply this information to the Registration Server
19 when requested by the a user interacting with an OBJECT.

20

21 Viewing OBJECTs, accessing property pages, and initiating other operations
22 discussed above, according to the invention, requires SYSTEM EXTENSION
23 functionality. Specifically, the SYSTEM EXTENSION acts as an extension to the
24 user's operating system, ensuring that required functionality is available from
25 within various applications and not just through an Internet browser. The SYSTEM
26 EXTENSION is preferably compact, self-installing, and freely distributed via the
27 Internet or as part of a customer's packaged solution.

28

29 As discussed above, the CONTAINER can be created by the Toolbox or
30 Express Packager. In creating the CONTAINER, the content owner, either by way of

1 the Toolbox or the Express Packager, associates Digital Creative Work with
2 Metadata, such as artistic or business attribution information (credits) and
3 permission parameters. It is intended that the invention operate with all standard
4 digital formats for the underlying source work, including GIF, JPEG, WAV, AVI,
5 and others. In one embodiment of the invention, the content owners edit the
6 Metadata values or properties using a set of Property Pages as an interface. The set
7 of required and optional properties for a particular OBJECT are defined by a
8 Template, created using the Template Editor. The Template also describes the visual
9 layout used in the property page presentation of the Metadata. A variety of
10 Templates may be created and applied to different types of content and for different
11 business or licensing models.

12
13 A content owner can also choose to create either registered or unregistered
14 CONTAINERS. In the case of unregistered OBJECTs, all content and Metadata
15 properties are stored in the CONTAINER itself. In the case of registered objects, the
16 Metadata properties are typically stored in two locations: within the CONTAINER
17 and remotely on a Registration Server. Properties stored within the CONTAINER
18 are referred to herein as static; properties that are retrieved from a Registration
19 Server are referred to herein as dynamic, since their values may change during the
20 life of the CONTAINER.

21
22 If the CONTAINER is to be registered, a Template supplied by the designated
23 Registration Server is used. That Template specifies the dynamic properties to be
24 supplied by the user that will be transferred to and stored in the Registration Server.
25 If an unregistered object is to be created, the content owner can select one of several
26 default Templates or he can create a custom Template that allows static attribution
27 information and communications with the creator/owner by email and web page
28 access only.

1 Registered CONTAINERS are better suited to content that is destined for
2 commercial use. Advantages of registration include authentication, ability to serve to
3 the user variable data such as terms for licensing, ability to change information after
4 distributing the object, and automated transactions. Unregistered CONTAINERS
5 may be desirable for material with a very short life cycle (e.g., weather maps), very
6 low value (e.g., vacation photos), or for non-commercial distribution where the user
7 simply wants to attach identifying information and facilitate email or web page
8 access.

9
10 The following are a few of the major features of CONTAINERS and OBJECTs,
11 as created by the invention:

- 12 • Viewing and Access - Objects can be rendered on systems where SYSTEM
13 EXTENSION functionality is installed.
- 14 • Restrictions - CONTAINERS encourage compliance with the Copyright Laws
15 by intercepting attempts to perform certain types of operations on the Digital
16 Creative Work (e.g., drag-and-drop, copy, save or print).
- 17 • Content - The CONTAINERS can contain all standard and commonly used
18 formats for image, sound, video, and text display.
- 19 • Property Pages - Property pages adhere to standard representations
20 consistent with the operating system and other applications. Static data is
21 displayed on pages. Also, for Registered Objects, dynamic data can be retrieved
22 on demand from a Registration Server.
- 23 • Other security measures, described above, can be used to ensure the integrity
24 of the CONTAINERS, preventing unauthorized and undetected modifications to
25 the content or METADATA.
- 26 • CONTAINERS provide the capability to initiate communications to a
27 creator/ owner through the following mechanisms:
 - 28 – Email - Email addresses can be stored in the CONTAINER's properties,
29 and email messages can be initiated when viewing the Object's property
30 pages. Email messages can be edited and transmitted a number of ways

- 1 including SMTP (direct Internet mail protocol), MAPI (Mail API) or by
2 launching a user's configured email client application (e.g., Eudora or
3 Microsoft Exchange).
- 4 – Web page access - URLs can be stored in the CONTAINER's properties,
5 and a web browser such as Netscape Navigator™ or Microsoft Internet
6 Explorer™ can be launched to access the specified page.
- 7 – Registration Server transactions - Registered CONTAINERS can initiate a
8 variety of transactions with a Registration Server. Transactions include the
9 retrieval of Dynamic Properties, the completion of a Permission Contract,
10 and payment for licensing fees. These transactions can be authenticated
11 using cryptographic techniques.

12
13 SYSTEM EXTENSION functionality provides the necessary functions to allow
14 a user to render an OBJECT and to access property pages and functions. It is
15 generally provided (e.g., "delivered") as an extension to the operating system. The
16 SYSTEM EXTENSION is intended to be widely and freely distributed online and
17 through traditional distribution media such as CD-ROMs and diskettes. Such
18 extensions should have the following properties:

- 19 • Compact - The Extensions will often be loaded electronically by a user through a
20 web-page or FTP server.
- 21 • Self-installing - The Extension can be installed with little or no interaction.
- 22 • Self-updating - Updates required for subsequent releases will be automatically
23 detected and installed.
- 24 • Backward Compatible - New Versions of the Extension will always be able to
25 view and use older OBJECTS.
- 26 • Forward Compatible - Objects with new formats and capabilities, created with
27 newer versions of the Toolbox and Express Packager, can be viewed with older
28 versions of the System Extension. The older System Extension can, for example,
29 ignore new features or functionality supported by the newer Objects. This is

1 analogous to viewing web pages using newer HTML extensions (e.g., tables or
2 frames) with older browsers.

3
4 The Registration Server is the storage and administrative facility for
5 registered CONTAINERS. A registration server is the primary component required
6 for organizations running a REGISTRY. A REGISTRY is, for example, analogous to a
7 Web site, except that instead of sending HTML pages and responding to requests
8 with the HTTP protocol, the REGISTRY is interacting across a network with
9 OBJECTS. A REGISTRY can include a batch or real-time link to an organization's
10 legacy permission or rights management system. The major functions of the
11 Registration Server can, without limitation, include:

- 12 • Object Registration - The Registration Server is the where the dynamic properties
13 for a registered CONTAINERS are stored. These properties can be updated by
14 the Registration Server administrator when necessary. Objects retrieving these
15 properties will immediately reflect the updated values.
- 16 • Template Creation - The Template Editor provides the operator of a registration
17 server with the ability to create and customize Templates, including the layout of
18 property pages and the definition of the static and dynamic properties to be
19 associated with Objects. Templates can be organized and grouped for
20 distribution to creators/owners for use with the Toolbox or the Express
21 Packager.
- 22 • Creator/Owner Registration - Several options are available for initiating a
23 relationship with a creator/owner depending upon the business model adopted
24 by the operator of a registration server. These options range from assigning a
25 simple user account name and password to a sophisticated high-security
26 procedure using officially certified digital signatures.
- 27 • External System Linkages - The Registration Server can interface to existing
28 rights management systems through one of several mechanisms:
 - 29 – The Express Packager allows one-way batch creation of Objects.

- 1 – The Packaging API allows real-time creation of Objects. The API is two-
2 way, enabling the update of data in the external system based on changes
3 made to the Registration Server.
- 4 – The Registration Server Database Mapper allows a direct interface from
5 the Server to an existing external database. The Mapper allows a flexible
6 mapping of the Object Properties to legacy systems.
- 7 • The Report Writer - Pre-formatted and customized reports are available,
8 including the following classes of reports:
 - 9 – Registered Object Reports
 - 10 – Creator/Owner Account Reports
 - 11 – Inquiry and Permission Transaction Reports
 - 12 – Server Activity Reports
 - 13 – Systems Operation Reports

14
15 One exemplary Registration Server schematic is shown in Figure 16.

16
17 The Registration Server also provides for certain problem situations that may
18 arise with Objects.

- 19 • Servicing Objects for which the Registration Server record has been removed or
20 transferred. If ownership has been transferred, then a transaction request may
21 simply be redirected to the appropriate server. A special "backstop" server can
22 be provided so that an Object contact the backstop server if all other attempts to
23 locate the appropriate Registration Server fail. This server includes a master
24 directory of Registration Servers. If the relationship between the creator and the
25 Registration Server has terminated, then an appropriate notification will be
26 returned.
- 27 • Servicing Objects which submit requests that for one reason or another violate an
28 authenticity check. If the server receives any unusual transaction requests,
29 including requests indicating an authentication failure, then an audit trail will be
30 maintained.

1

2 The Administration Server is an add-on component for operators of the
3 Registration Server. The Administration Server, for example, serves small
4 publishers, service bureaus, and independent professionals who do not have existing
5 methods for administering royalties, handling on-line financial transactions, and
6 reporting on the financial and administrative activity of the system. The
7 Administration Server brings some of the necessary publishing functionality to the
8 small user.

9

10 As discussed above, the packaging process associates Metadata with Digital
11 Creative Works and instantiates the CONTAINER as an Object. In one method of the
12 invention, the METADATA is displayed by means of its property pages; the
13 properties required on these pages and their layout is specified by the object's
14 property page template. Templates can be used for both registered and unregistered
15 Objects, but are of special importance when an OBJECT is registered.

16

17 The Template Editor enables the operator of a Registration Server to create
18 and customize templates, including the layout of property pages and the definition
19 of the static and dynamic properties to be associated with Objects. Templates may be
20 organized and grouped for distribution to creators and owners for use with the
21 Toolbox or the Express Packager. The Template Editor preferably has a GUI with a
22 palette-oriented desktop motif consistent with current visual software design tools
23 (e.g.: Visual Basic).

24

25 A Template contains a hierarchy of data items, including, without limitation,
26 the following:

- 27 • A collection of property pages.
- 28 • For each property page, a collection of controls that will appear on that page.
- 29 • For each property page, a collection of property sets. A property set is a collection
30 of property descriptors that define the attributes of each property.

- 1 • The definition of the template's home Registration Server.
- 2 • The definition of the template's connection object.

3
4 The Template Editor gives the user the tools to define property sets and their
5 associated property descriptors. Each descriptor is uniquely identified upon
6 creation. Each property page interface is built from a set of controls. The user selects
7 each control from a palette and draws on a form in a fashion similar to Visual Basic.
8 For each control selected, the user can define a new property descriptor to be
9 associated with the control or may select from a set of "hard-coded" routines that the
10 selected control can execute. Each control is assigned a unique identifier upon
11 creation.

12
13 After the user has created property pages and property sets, the user can save
14 everything as a Template that can be inserted into another Template Editor project.
15 Alternatively they may save the work as a bound template that can be used directly
16 by a packaging tool to create Objects. Prior to saving the user's work as a bound
17 Template, the Template Editor automatically generates an input data form that may
18 be optionally edited. When saving as a bound template, the template editor
19 generates a fixed-format input data file that will be parsed by the PACKAGER.

20
21 The Express Packager is used by content owners who convert large amounts
22 of content into CONTAINERS by automatically merging Metadata and Digital
23 Creative Work. The Express Packager creates registered and unregistered Objects
24 and generally has two modes of operation:

- 25 • Conversion Mode enables large numbers of existing digital files to be converted
26 into CONTAINERS. When operating in conversion mode, the Express Packager
27 actively gets the content and the input data file that describes the Metadata and
28 creates the CONTAINER. Data is either retrieved from a database or from a text
29 file or other intermediate container storing the pertinent information.

- 1 • Creation Mode enables the Express Packager to operate under the control of
2 another program through the real-time Packaging API (LPAPI). In this way, the
3 Express Packager operates in a passive mode, taking its instructions from other
4 applications. This mode is appropriate for packaging content that is created in
5 real-time such as the output from Java applications, CGI scripts, proprietary
6 publishing applications, etc.

7
8 The LPAPI can be made available through an OLE Automation interface to
9 enable a flexible and industry-standard protocol used to create and register Objects.
10 The LPAPI allows custom interactive or batch interfaces to be built using a large
11 array of development and scripting tools such as Visual Basic, C++, Microsoft Office
12 applications, and other similar applications.

13
14 The LPAPI can also be made available "off the shelf" for use in applications
15 such as web servers (CGI, ISAPI), browsers (Java, ActiveX, plug-ins) and third party
16 programs such as creativity tools and multimedia development systems.

17
18 The Toolbox can be used by content owners to interactively create
19 CONTAINERS. The Toolbox focuses on ease-of-use through an intuitive interface
20 with on-line help, wizards, and other supporting mechanisms. The Toolbox can
21 create registered and unregistered CONTAINERS. The Toolbox combines Templates
22 provided by the Registry for registered objects, or by other means for unregistered
23 objects. Some Registries can choose to use standard Templates. The Template Editor
24 is useful, for example, for creators who are using Registries that allow Objects to be
25 registered with custom templates that are derived from those supplied by the
26 Registry. This provides the Registry with the capacity to allow creators to add
27 additional properties that complement those required by the Registry. The Toolbox
28 can use cryptographic techniques to ensure the integrity of the CONTAINER and to
29 provide two-way authentication of the parties involved in object registration.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

The invention thus attains the objects set forth above, among those apparent from preceding description. Since certain changes may be made in the above apparatus and methods without departing from the scope of the invention, it is intended that all matter contained in the above description or shown in the accompanying drawing be interpreted as illustrative and not in a limiting sense.

It is also to be understood that the following claims are to cover all generic and specific features of the invention described herein, and all statements of the scope of the invention which, as a matter of language, might be said to fall there between.

Having described the invention, what is claimed is:

- 1 1. A method of packaging a digital creative work, comprising the steps of:
2 encapsulating the work within a data container; encapsulating metadata within the
3 container; and integrating, with the container, means for accessing the work and the
4 metadata.
5
- 6 2. A method according to claim 1, wherein the step of integrating means for
7 accessing the work further comprises the step of integrating, with the container,
8 means for rendering the work.
9
- 10 3. A method according to claim 2, wherein the step of integrating means for
11 rendering the work further comprises the step of integrating, with the container,
12 means for printing the work.
13
- 14 4. A method according to claim 2, wherein the step of integrating means for
15 rendering the work further comprises the step of integrating, with the container,
16 means for copying the work.
17
- 18 5. A method according to claim 2, wherein the step of integrating means for
19 rendering the work further comprises the step of integrating, with the container,
20 means for viewing the work.
21
- 22 6. A method according to claim 1, wherein the step of integrating means for
23 accessing the work further comprises the step of integrating, with the container,
24 means for controlling use of the work.
25
- 26 7. A method according to claim 1, wherein the step of integrating means for
27 accessing the work further comprises the step of integrating, with the container,
28 means for limiting use of the work.
29

1 8. A method according to claim 1, wherein the step of integrating means for
2 accessing the work further comprises the step of integrating, with the container,
3 means for disallowing use of the work.
4

5 9. A method according to claim 1, wherein the step of integrating means for
6 accessing the work and the metadata further comprises the step of integrating, with
7 the container, means for operating on the metadata.
8

9 10. A method according to claim 9, wherein the step of integrating means for
10 operating on the metadata further comprises integrating, with the container, means
11 for providing email to one or more external addresses.
12

13 11. A method according to claim 9, wherein the step of integrating means for
14 operating on the metadata further comprises integrating, with the container, means
15 for providing web access to one or more WWW addresses.
16

17 12. A method according to claim 9, wherein the step of integrating means for
18 operating on the metadata further comprises integrating, with the container, means
19 for providing interactive licensing to the work.
20

21 13. A method according to claim 9, wherein the step of integrating means for
22 operating on the metadata further comprises integrating, with the container, means
23 for providing a link to a digital contract for the work.
24

25 14. A method according to claim 9, wherein the step of integrating means for
26 operating on the metadata further comprises integrating, with the container, means
27 for displaying descriptive information.
28

29 15. A method according to claim 14, wherein the descriptive information
30 comprises one or more of the following: authorship information, historical

1 information, ownership information, date information, time information, and
2 bibliographic information.

3
4 16. A method according to claim 14, wherein the descriptive information
5 comprises a digital signature to verify authenticity of the work.

6
7 17. A method according to claim 9, wherein the step of integrating means for
8 operating on the metadata further comprises integrating, with the container, means
9 for updating the metadata.

10
11 18. A method according to claim 1, further comprising the step of forming the
12 data container as a plurality of associated data that are distributed across one or
13 more of the following: a computer network, an Internet, a LAN, a WAN, an on-line
14 service, and an Intranet.

15
16 19. A method according to claim 1, wherein the work is selected from the group
17 of digital images and graphics, digital photos, digital audio, digital video, digital
18 music sequences, word processing files, spreadsheet files, and mixtures thereof.

19
20 20. A method according to claim 19 wherein the digital images and graphics are
21 selected from the group of JPEG, GIF, BMP, TIFF and mixtures thereof.

22
23 21. A method according to claim 19 wherein the digital audio is selected from the
24 group of WAV, SND, AIFF, AU and mixtures thereof.

25
26 22. A method according to claim 19 wherein the digital music sequence
27 comprises MIDI.

28
29 23. A method according to claim 19 wherein the digital video is selected from the
30 group of AVI, MOV, MPEG and mixtures thereof.

1

2 24. A method according to claim 19 wherein the word processing files are
3 selected from the group of files created through Microsoft Word™, Novell
4 WordPerfect™ and mixtures thereof.

5

6 25. A method according to claim 19 wherein the spreadsheet files comprise files
7 created through Microsoft Excel™.

8

9 26. A method according to claim 1, wherein the step of encapsulating metadata
10 further comprises the step of encapsulating copyright management information.

11

12 27. A method according to claim 26, wherein the copyright management
13 information comprises any of ownership identification information, ownership
14 contact information, rights administration information, rights administration contact
15 information, creatorship information, authorship information, creator contact
16 information, author contact information, listings of antecedent object information,
17 listings of related object information, licensing terms, licensing conditions, publisher
18 information, and ownership credits.

19

20 28. A method according to claim 27, wherein any of the ownership contact
21 information, rights administration contact information, creator contact information,
22 author contact information comprise email addresses, web access addresses, and
23 mixtures thereof.

24

25 29. A method according to claim 1, wherein the step of encapsulating metadata
26 further comprises the step of encapsulating registration data, the registration data
27 identifying an associated registration server capable of administering the data
28 container.

29

1 30. A method according to claim 29, wherein the metadata is modifiable and
2 accessible through on-line communication with the registration server.

3
4 31. A method according to claim 30, further comprising the step of storing at least
5 part of the metadata at a database of the registration server.

6
7 32. A method according to claim 30, further comprising the step of down-loading
8 at least part of the metadata from the registration server.

9
10 33. A method according to claim 1, wherein the step of integrating means for
11 accessing the metadata comprises providing a user interface to the data container to
12 review at least part of the metadata on a computer.

13
14 34. A method according to claim 33, wherein the the user interface is displayable
15 on the computer and is selectable by a user of the computer to modify information
16 therein.

17
18 35. A method according to claim 1, wherein the step of encapsulating metadata
19 further comprises the step of encapsulating, with the data container, minimum
20 permissions data, the minimum permissions data specifying one or more operations
21 that can be performed on the work without a license to the work.

22
23 36. A method according to claim 1, wherein the step of encapsulating metadata
24 further comprises the step of encapsulating, with the data container, minimum
25 permissions data, the minimum permissions data specifying a default contract to the
26 work, the default contract specifying a minimum set of operations that can be
27 performed by applications on the work.

28

1 37. A method according to claim 35 or 36, wherein the operations are selected
2 from the group of drag and drop operations, printing operations, editing
3 operations, activating operations, saving operations, and viewing operations.
4

5 38. A method according to claim 1, wherein the step of integrating means for
6 accessing the work and the metadata further comprises the step of integrating, with
7 the container, one or more of the following: means for encoding the metadata, means
8 for compressing the metadata, means for manipulating the metadata, means for
9 encrypting the metadata, means for decoding the metadata, and means for
10 decrypting the metadata.
11

12 39. A method according to claim 1, wherein the step of integrating means for
13 accessing the work and the metadata further comprises the step of integrating, with
14 the container, one or more of the following: means for encoding the work, means for
15 compressing the work, means for manipulating the work, means for encrypting the
16 work, means for decoding the work, and means for decrypting the work.
17

18 40. A method according to claim 1, wherein the step of encapsulating the work
19 further comprises the step of encrypting the work.
20

21 41. A method according to claim 1, wherein the step of encapsulating metadata
22 further comprises the step of associating a metadata template with the container, the
23 metadata template describing registration with a registration server.
24

25 42. A method according to claim 1, wherein the step of encapsulating metadata
26 further comprises the step of associating a metadata template with the container, the
27 metadata template specifying properties of the container used to register the
28 container with a registration server.
29

1 43. A method according to claim 42, wherein the step of encapsulating metadata
2 further comprises specifying, within the template, a display interface used to view
3 the properties.

4

5 44. A method according to claim 1, wherein the step of encapsulating metadata
6 further comprises the step of associating a metadata template with the container, the
7 metadata template identifying user-selectable optional properties of the container.

8

9 45. A method according to claim 1, wherein the step of encapsulating metadata
10 further comprises the step of associating a metadata template with the container, the
11 metadata template specifying requirements and rules associated with the work.

12

13 46. A method according to claim 41, 44 or 45, further comprising the step of
14 providing, with the metadata template, a user interface suitable for viewing
15 information related to the metadata and the work.

16

17 47. A method according to claim 41, 42, 44 or 45, further comprising the step of
18 providing different metadata templates corresponding to different types of works.

19

20 48. A method according to claim 41, 42, 44 or 45, further comprising the step of
21 providing different metadata templates corresponding to different licensing models.

22

23 49. A method according to claim 1, wherein the step of encapsulating metadata
24 further comprises the step of associating, with the container, operations that can be
25 performed on the work.

26

27 50. A method according to claim 1, further comprising the step of registering the
28 document with one or more registration servers, each registration server providing
29 on-line administration of the container and having user-selectable registration

1 templates for associating metadata with the container, at least part of the metadata
2 being modifiable over a lifetime of the container.

3
4 51. A method according to claim 1, wherein the step of encapsulating metadata
5 further comprises the step of associating, with the container, requirements of specific
6 parties having rights in or to the work.

7
8 52. A method according to claim 1, wherein the requirements comprise a
9 requirement to obtain a license to the work prior to additional use of the work.

10
11 53. A method according to claim 1, wherein the requirements comprise a
12 requirement of obtaining information about entities desiring access to the work.

13
14 54. A method according to claim 53, wherein the information comprises address
15 and billing information of the entities.

16
17 55. A method according to claim 53, wherein the entities comprise one or more of
18 an individual, a partnership, a company, a government agency, and an educational
19 institution.

20
21 56. A method according to claim 1, wherein the step of encapsulating metadata
22 further comprises the step of encapsulating information indicative of one or both of
23 an owner and creator of the media, and further comprising the step of
24 communicating with one or both of the owner and creator through one or both of
25 email and web page access.

26
27 57. A method according to claim 1, wherein the steps of encapsulating are made
28 through object-based technology.

1 58. A method according to claim 1, wherein the container comprises object-based
2 technology.

3
4 59. A method according to claim 57 or 58, wherein the object-based technology
5 comprises one or more of OLE™, ActiveX™, OpenDoc™, and hybrid
6 OLE™/OpenDoc™.

7
8 60. A method of accessing a digital creative work, comprising the steps of:
9
10 installing a system extension onto a computer, the extension including (i) means for
11 operating in conjunction with an operating system controlling the computer; (ii)
12 means for accessing a data container having the work and metadata, including
13 minimum permissions data, attached thereto, the minimum permissions data
14 specifying one or more operations that can be performed on the work without a
15 license to the work; and (iii) means for recognizing the minimum permissions data
16 and for enabling a user of the computer to use the work in accord with the specified
17 operations; and

18
19 accessing the container and using the work in accord with the specified operations.
20

21 61. A method according to claim 60, wherein the step of installing a system
22 extension further comprises the step of distributing the extension to the computer
23 with a computer operating system.

24
25 62. A method according to claim 60, wherein the step of installing a system
26 extension further comprises the step of distributing the extension to the computer
27 from one or more content provider sites, the content provider sites creating the
28 media.
29

1 63. A method according to claim 60, wherein the step of installing a system
2 extension further comprises the step of distributing the extension to the computer
3 with creativity tools.

4
5 64. A method according to claim 63, wherein the step of distributing the
6 extension comprises utilizing image and graphic creativity tools selected from the
7 group of Adobe Photoshop™, Fractal Design Painter™, CorelDraw.

8
9 65. A method according to claim 63, wherein the step of distributing the
10 extension comprises utilizing multimedia authoring tools selected from the group of
11 Macromedia Director™, Macromedia Authorware™, Asymetrix Toolbook™,
12 Aimtech IconAuthor™.

13
14 66. A method according to claim 63, wherein the step of distributing the
15 extension comprises utilizing web authoring tools selected from the group of
16 Microsoft FrontPage™, Adobe PageMill™, Adode SiteMill™, SoftQuad HoTMetaL
17 Pro™, Corel Web.Designer™.

18
19 67. A method according to claim 63, wherein the step of distributing the
20 extension comprises utilizing sound editing tools selected from the group of
21 Macromedia SoundEdit Pro™ and DigiDesign Pro Tools™.

22
23 68. A method according to claim 63, wherein the step of distributing the
24 extension comprises utilizing video editing tools selected from the group of Avid
25 Media Suite™, Asymetrix Digital Video Producer™, Adobe
26 Premiere™.

27
28 69. A method according to claim 63, wherein the creativity tools comprise one or
29 more of the following: Microsoft Word™, Microsoft Excel™, Microsoft
30 Powerpoint™, and Novell WordPerfect™.

1

2 70. A method according to claim 60, wherein the step of installing a system
3 extension further comprises the step of distributing the extension to the computer
4 with web browsers selected from the group of Netscape Navigator™ and Microsoft
5 Internet Explorer™.

6

7 71. A method according to claim 60, wherein at least part of the container is
8 stored in a remote database, and further comprising the step of accessing at least
9 part of the container through on-line communication with the database.

10

11 72. A method according to claim 71, wherein the step of accessing part of the
12 container through on-line communication comprises one or more of the following:
13 communication through the Internet, communication through a computer network,
14 and communication through the Intranet.

15

16 73. A method according to claim 71, wherein the step of accessing part of the
17 container through on-line communication comprises utilizing a file data stream
18 wherein rendering of the work is possible only after all data representative of the
19 work is present at the computer.

20

21 74. A method according to claim 71, wherein the step of accessing part of the
22 container through on-line communication comprises utilizing a continuous data
23 stream wherein rendering of the work is possible, in part, with concurrent arrival, at
24 the computer, of data representative of the work.

25

26 75. A method according to claim 60, wherein at least part of the container is
27 stored on a CD-ROM, and further comprising the step of accessing the part of the
28 container through communication with a CD-ROM drive.

29

1 76. A method according to claim 60, wherein the at least part of the container is
2 stored on a magnetic data disk, and further comprising the step of accessing part of
3 the container through communication with a disk drive.
4

5 77. A method according to claim 60, wherein at least part of the container is
6 stored within internal memory of the computer, and further comprising the step of
7 accessing part of the container within internal memory.
8

9 78. A method according to claim 60, wherein the extension comprises means for
10 recognizing registration data within the metadata, the registration data identifying
11 an associated registration server capable of administrating the data, and further
12 comprising the step of contacting the registration server to negotiate, on-line, a
13 license to the work.
14

15 79. A method according to claim 78, further comprising the step of contacting the
16 registration server to negotiate for auxiliary permissions data, the auxiliary
17 permissions data specifying auxiliary uses of the media that is licensed beyond the
18 authorized use specified in the minimum permissions data.
19

20 80. A method according to claim 79, wherein the extension further comprises
21 means for recognizing the auxiliary permissions data and for enabling the user to
22 use the work in accord with the auxiliary uses.
23

24 81. A method according to claim 60, wherein the extension comprises means for
25 recognizing registration data within the container, the registration data identifying
26 an associated registration server capable of administrating the data, and further
27 comprising the step of contacting the registration server to authenticate the work.
28

- 1 82. A method according to claim 60, wherein the extension further comprises
2 means for prohibiting unauthorized uses of the work when the unauthorized uses
3 exceed the operations specified in the minimum permissions data.
4
- 5 83. A method according to claim 82, wherein the means for prohibiting
6 unauthorized uses of the media comprises means for prohibiting drag-and-drop
7 operations on the computer.
8
- 9 84. A method according to claim 82, wherein the means for prohibiting
10 unauthorized uses of the media comprises means for prohibiting one or more of
11 copying, saving and printing the work.
12
- 13 85. A method according to claim 60, further comprising the step of acquiring
14 auxiliary permissions data for the container, the auxiliary permissions specifying a
15 set of operations that can be performed on the work after executing a digital contract
16 to the work.
17
- 18 86. A method according to claim 85, further comprising the step of acquiring
19 auxiliary permissions data through one of email or web access.
20
- 21 87. In an operating system of the type which facilitates control and
22 communication of a digital data processor, the improvement comprising a plug-in
23 extension for manipulating copyrighted electronic media, the extension comprising
24 means for opening a data container having a digital creative work and minimum
25 permissions data attached thereto, the minimum permissions data specifying one or
26 more operations that can be performed on the work without a license to the work,
27 the extension recognizing the minimum permissions data and enabling a user of the
28 processor to use the work in accord with the specified operations.
29

1 88. In an operating system of claim 87, the further improvement wherein the
2 container has metadata attached thereto, the metadata being selected from the group
3 of ownership identification information, ownership contact information, rights
4 administration information, rights administration contact information, creatorship
5 information, authorship information, creator contact information, author contact
6 information, listings of antecedent object information, listings of related object
7 information, licensing terms, licensing conditions, publisher information, and
8 ownership credits, and wherein the extension comprises means for reviewing the
9 metadata selectively.

10
11 89. A plug-in operating system extension, comprising:

12
13 means for operating in conjunction with an operating system controlling a digital
14 data processor;

15
16 means for recognizing a data container having digital creative works and minimum
17 permissions data attached thereto, minimum permissions data specifying one or
18 more operations that can be performed on the work without a license to the work;
19 and

20
21 means for opening the container and enabling a user of the processor to use the
22 work in accord with the specified operations.

23
24 90. A plug-in extension according to claim 89, further comprising means for
25 decrypting the media.

26
27 91. A plug-in extension according to claim 89, wherein the container has
28 registration information attached thereto, the registration information specifying a
29 registration server capable of administering the container, and further comprising

1 means for recognizing the registration information and for communicating with the
2 registration server to acquire properties associated with the container.

3
4 92. A plug-in extension according to claim 89, wherein the container has
5 registration information attached thereto, the registration information specifying a
6 registration server capable of administering the document, and further comprising
7 means for negotiating a digital contract with the registration server, the contract
8 specifying licensing terms and auxiliary uses to the work.

9
10 93. A server for managing digital copyrighted works, comprising:

11
12 (A) means for communicating with at least one on-line data processor connected
13 for communication with the server, the on-line data processor having (i) means for
14 recognizing a secure digital document having copyrighted electronic media and
15 minimum permissions data attached thereto, the minimum permissions data
16 specifying minimum authorized use of the media without a license to the media; and
17 (ii) means for opening the document and enabling a user of the processor to use the
18 media in accord with the authorized use;

19
20 (B) means for registering the document according to user-selected options at the
21 data processor; and

22
23 (C) means for negotiating with the data processor to obtain auxiliary permissions
24 to the document and for sending the auxiliary permissions data to the data processor
25 thereby expanding the authorized use of the data processor.

26
27 94. A method for managing copyrighted electronic media, comprising the steps
28 of:

- 1 formatting the media into a secure electronic container, the container including a
2 digital representation of the media and a minimum permissions data set specifying
3 the minimum authorized use of the media;
4
5 registering the electronic media on a server and assigning a registration identifier to
6 the container, the server being connected for on-line data transfers with at least one
7 computer;
8
9 transmitting licensing terms from the server to the computer in response to a request
10 to license the media; and
11
12 augmenting the permissions data set with auxiliary permissions when the computer
13 indicates acceptance of the terms, the auxiliary permissions providing authorization
14 to utilize the media beyond what is authorized in the minimum permissions data
15 set.
16
- 17 95. A method according to claim 94, further comprising the step of determining
18 whether the computer's use of the media is authorized by the permissions data set.
19
- 20 96. A method according to claim 94, further comprising the step of enabling
21 limited use of the media at the computer, the limited use corresponding to the
22 minimum permissions data set.
23
- 24 97. A method according to claim 94, further comprising the step of verifying that
25 a user of the computer is an authorized user, the step of verifying occurring before
26 the computer requests a license to the server.
27
- 28 98. A method according to claim 97, wherein the step of verifying includes the
29 step of searching for the user's public key with a certification stamp from a
30 certification authority.

1

2 99. A method according to claim 94, wherein the step of formatting the media
3 further comprises the step of including sourceworks extensions within the container,
4 the sourceworks extensions providing a bibliographic record of the media.

5

6 100. A method according to claim 94, further comprising the step of providing,
7 through the server, selected transactional information, the information including at
8 least one of (i) a number of registrations at the server and (ii) a quantitative
9 indication of licensing revenues generated through the server.

10

11 101. A system for authorizing access to copyrighted electronic media, comprising
12 an authorization server connected for data transfer between an internal memory and
13 at least one external data processor, the server having

14

15 (A) first storage means for storing selected information about the electronic media;

16

17 (B) relay means, responsive to a request signal by the data processor, for
18 communicating the selected information to the data processor; and

19

20 (C) data comparison means for receiving response signals from the data processor
21 and comparing the selected information with the response signals, the data
22 comparison means generating an acceptance signal when the response signals
23 correspond to at least a part of the selected information, and communicating the
24 acceptance signal to the data processor to authorize access to the media.

25

26 102. A system according to claim 101, wherein the selected information comprises
27 a digital representation of at least one of (i) a copyright ownership of the media, (ii)
28 a set of licensing terms for the media for different user classifications, and (iii)
29 revenue estimates about the media.

1
2 103. A system according to claim 101, further comprising memory means for
3 storing the electronic media.

4
5 104. A system according to claim 103, further comprising electronic media stored
6 within the memory means, the media being a digital representation of at least one of
7 (i) literary work, (ii) musical work, (iii) dramatic work, (iv) choreographic work, (v)
8 pictorial work, (vi) audiovisual work, (vii) a sound recording, and (viii) architectural
9 work.

10
11 105. A system according to claim 104, wherein the media is encrypted.

12
13 106. A system according to claim 104, further comprising data header means for
14 storing selected header information about the media, the header information being a
15 digital representation of at least one of (i) a unique file format, (ii) a document
16 format revision code, (iii) a creator application type, (iv) a media data type, and (v) a
17 comment field.

18
19 107. A system according to claim 104, further comprising means for storing an
20 unencrypted header for uniquely identifying the electronic media.

21
22 108. A system according to claim 104, further comprising means for storing a data
23 identifier, the data identifier specifying selected registration information about the
24 electronic media.

25
26 109. A system according to claim 108, wherein the data identifier comprises a
27 digital representation of at least one of (i) a registration code uniquely identifying
28 the server, and (ii) a registration number uniquely identifying the media in the
29 internal memory.

1

2 110. A system according to claim 104, further comprising means for tagging an
3 encrypted digital signature to the media, the signature providing subsequent
4 authentication of the media.

5

6 111. A system according to claim 104, further comprising means for appending
7 minimum permissions to the media, the minimum permissions forming a digital
8 representation that specifies a minimum authorized use of the media.

9

10 112. A system according to claim 111, wherein the authorized use comprises a
11 license to view the media.

12

13 113. A system according to claim 104, further comprising auxiliary permission
14 means for appending use restrictions the media selectively, the use restrictions
15 forming a digital representation that authorizes auxiliary uses of the media.

16

17 114. A system according to claim 101, further comprising a sourceworks extension
18 module for storing a bibliographic record of the media, the bibliographic record
19 forming a digital representation that specifies authorship information and the access
20 restrictions associated with the media.

21

22 115. A system according to claim 101, further comprising access control means for
23 withholding access authorization to a portion of the media, the access control means
24 being responsive to the acceptance signal to remove access restrictions to the
25 portion.

26

27 116. A system according to claim 101, wherein the server comprises means for
28 communicating with the data processor in accord with a TCP/IP network protocol.

29

- 1 117. A method for authorizing data transfers of copyrighted digital media,
2 comprising the steps of:
3
4 affixing content-specific permission information to the media, the permission
5 information specifying actions which are restricted and require augmented access
6 privileges to perform;
7
8 storing selected information about the electronic media on an authorization server
9 connected for data transfer with at least one computer;
10
11 electronically communicating selected information about the media to the computer;
12
13 receiving response signals from the computer and comparing the selected
14 information with the response signals; and
15
16 generating an acceptance signal when the response signals correspond to at least a
17 part of the selected information, thereby authorizing access to the media.
18
- 19 118. A method according to claim 117, wherein the step of communicating selected
20 information comprises the step of communicating a digital representation of at least
21 one of (i) a copyright ownership of the media, (ii) a set of licensing terms for the
22 media for different user classifications, and (iii) revenue estimates about the media.
23
- 24 119. A method for maintaining an electronic bibliographic record of digital media,
25 comprising the steps of:
26
27 opening an object container containing the digital media, the object container
28 including a representation of the media, a data identifier of media, and data
29 specifying minimum permissions required to access the media;

1
2 editing the digital media in an application environment; and

3
4 attaching the data identifier and minimum permissions data to the edited media into
5 a sourceworks list, the sourceworks list thereby providing a bibliographic record of
6 the media.

7
8 120. A method according to claim 119, wherein the container further includes
9 auxiliary permissions data specifying subsequent use authorizations to the media,
10 and further comprising the step of modifying the minimum permissions data such
11 that the minimum permissions data and auxiliary permissions data are viewable to
12 subsequent potential users of the media.

13
14 121. A method for determining the authenticity of digital media, comprising the
15 steps of formatting the media into a secure electronic container, the container
16 including a digital representation of the media and a minimum permissions data set
17 specifying the minimum authorized use of the media, and affixing an encrypted
18 digital signature to the media, the signature representing a registration of the media
19 and providing authentication to the media.

20
21 122. A computer network for managing original works of authorship, comprising:
22
23 means for affixing copyright information to a binary data element corresponding to
24 an authored media;

25
26 means for affixing minimum permissions information to the data element, the
27 permission information specifying a minimum authorized use of the data element;

1 a server for providing authorizations to the data element, the server including a
2 control module for transacting licenses with one or more computers networked with
3 the server; and

4
5 means for tagging the data element with auxiliary permissions, the auxiliary
6 permissions specifying the maximum authorized use of the media.

7
8 123. A system according to claim 122, further comprising means for maintaining
9 copyright information through derivative uses of the data element on the network.

10
11 124. A computer network according to claim 29, wherein the means for tagging
12 comprises means for appending identifying information to the data element, the
13 identifying information being selected from a digital representation of at least one of
14 (i) a source of the data element, (ii) a registry of the data element, (iii) a format of the
15 data, (iv) a transmission history of the data element; (v) a derivative minimum
16 permission data set for subsequent restricted access to the data on the network; (vi) a
17 digital signature of an author of the data element to provide an authenticity to the
18 data element, (vii) a copyright ownership of the data item, (viii) licensing detail
19 about the data element, and (ix) revenue detail about the data element.

20
21 125. A system for packaging electronic media within a secure digital document,
22 comprising:

23
24 means for enclosing the media as a binary data object within a data container;

25
26 means for attaching identification data to the data container; and

27
28 means for attaching minimum permissions data to the data container, the minimum
29 permissions data specifying minimum uses authorized for the media without a
30 license to the media,

1
2 the data container, identification data, and minimum permissions thereby forming
3 the digital document.
4

5 126. A system according to claim 125, further comprising means for attaching a
6 digital signature to the data container, the digital signature providing an
7 authentication to the media.
8

9 127. A system according to claim 125, further comprising means for encrypting the
10 media.
11

12 128. A system according to claim 125, further comprising means for affixing source
13 works extensions to the data container, the source works extensions specifying a
14 bibliographic record of the media, thereby providing persistence through
15 generations of derivative use of the media.
16

17 129. A system according to claim 125, further comprising auxiliary permission
18 means for appending use restrictions the data container, the use restrictions forming
19 a digital representation that extends the set of authorized uses available to a user of
20 the media.
21

22 130. A system according to claim 125, further comprising data header means for
23 storing selected header information about the media, the header information being a
24 digital representation of at least one of (i) a unique file format, (ii) a document
25 format revision code, (iii) a creator application type, (iv) a media type, and (v) a
26 comment field.
27

28 131. A system according to claim 125, further comprising means for storing an
29 unencrypted header for uniquely identifying the electronic media.

1

2 132. A system according to claim 125, further comprising means for storing a data
3 identifier, the data identifier specifying selected registration information about the
4 electronic media.

5

6 133. A system according to claim 132, wherein the data identifier comprises a
7 digital representation of a registration code uniquely identifying a server, and a
8 registration number uniquely identifying the media on the server.

9

10 134. A system according to claim 125, further comprising means for packaging the
11 media from within one of (i) a stand-alone software module, (ii) a plug-in software
12 module corresponding to an application environment that generated or modified the
13 media, (iii) a program extension corresponding to an application environment which
14 generated or modified the media, (iii) a software module integrated into an
15 application environment by way of a source code library or linkable object code
16 performing substantially similar functions.

17

18 135. A system for unpackaging electronic media configured within a secure
19 electronic container, comprising:

20

21 means for recognizing permissions data attached to the media, the permissions data
22 specifying one or more authorizations needed to electronically access the media; and

23

24 means for utilizing the media in a manner corresponding to the minimum
25 permissions when a user has the requisite authorizations to do so.

26

27 136. A system according to claim 135, further comprising means for engaging an
28 authorization server when the user does have the requisite authorizations.

29

1 137. A system according to claim 136, further comprising (A) means for
2 electronically transacting a license with the server, and (B) means for receiving, from
3 the server, auxiliary permission to utilize the media.

4
5 138. A system according to claim 135, further comprising means for interpreting a
6 digital signature attached to the media, the digital signature providing an
7 authentication of the media.

8
9 139. A method for protecting electronic media, comprising the steps of:

10
11 packaging the electronic media within a secure electronic container by (i) attaching a
12 data identifier to the media, and (ii) attaching data specifying minimum permissions
13 required to use the media;

14
15 registering the container on a server connected for data transfer with at least one
16 data processor; and

17
18 transferring auxiliary permissions from the server to the data processor upon
19 acceptance of licensing terms associated with the media.

20
21 140. A method according to claim 139, wherein the step of packaging the media
22 includes the step of encrypting the media.

23
24 141. A method according to claim 140, comprising the further step of encrypting
25 the media through an RSA public key algorithm.

26
27 142. A method according to claim 139, further comprising the step of transferring
28 the container to the data processor via one of point-to-point email, CD-ROM, ftp,
29 gopher, snmp, and http.

1
2 143. A method according to claim 139, comprising the further step of
3 communicating with the data processor in accord with TCP/IP network protocol.
4

5 144. A method according to claim 139, comprising the further the step of affixing
6 an encrypted digital signature to the media, the signature corresponding to a
7 registration of the media to provide authentication to the media.
8

9 145. A method according to claim 139, comprising the further the step of affixing
10 use restrictions to the media selectively, the use restrictions forming a digital
11 representation that is readable by the data processor to restrict subsequent access to
12 the media by a second data processor connected on the network.
13

14 146. A system for registering copyrighted electronic media, comprising an
15 authorization server connected for data transfer between an internal memory and at
16 least one external data processor, the server having
17

18 (A) request means for receiving a request signal from the data processor, the request
19 signal representing a request to register the media on the server;
20

21 (B) authentication means for determining the authenticity of the media and the data
22 processor based upon information about the media and the request signal; and
23

24 (C) means generating an acceptance signal when the media is authenticated,
25 thereby indicating that the server accepts the media for registration.

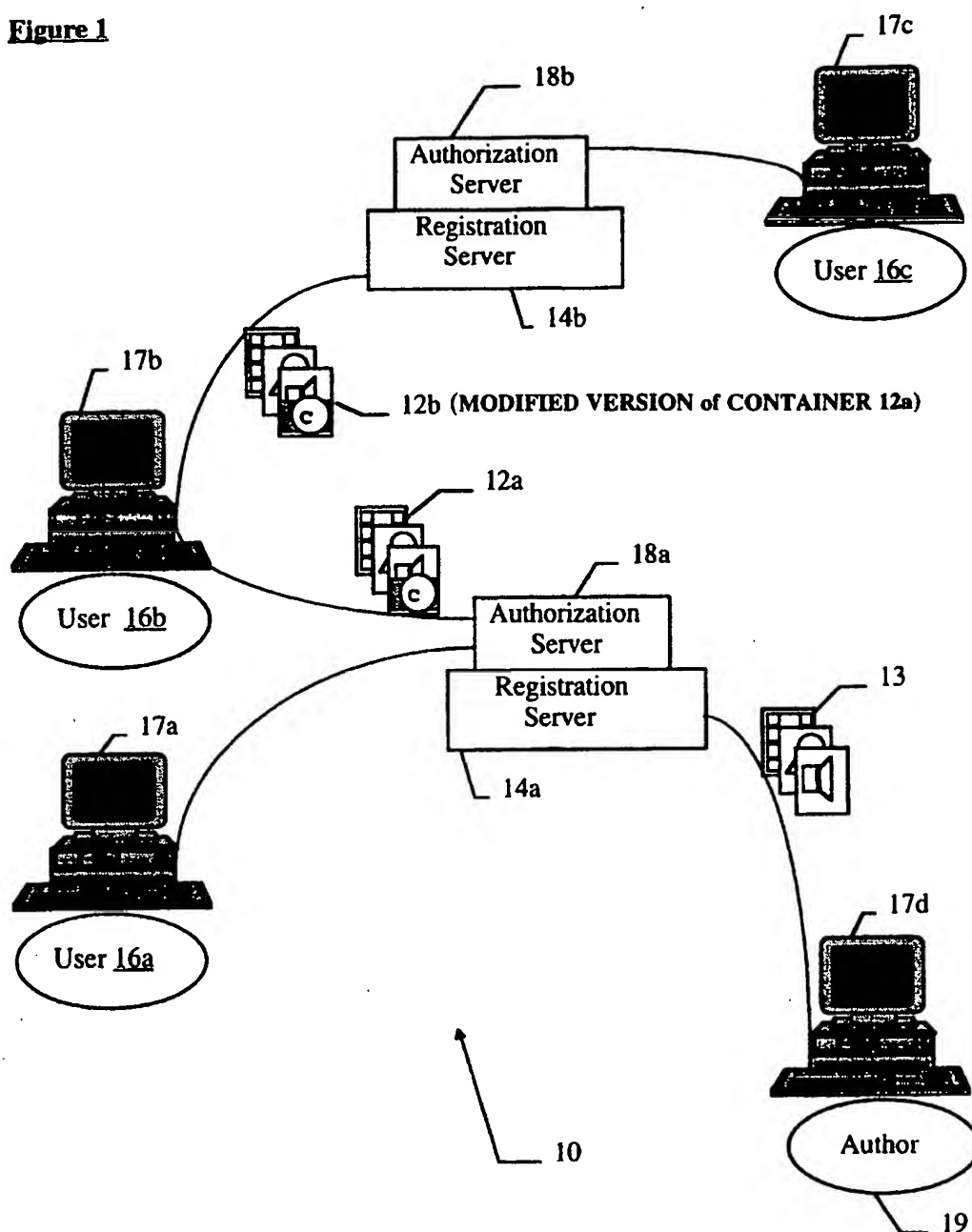
Figure 1

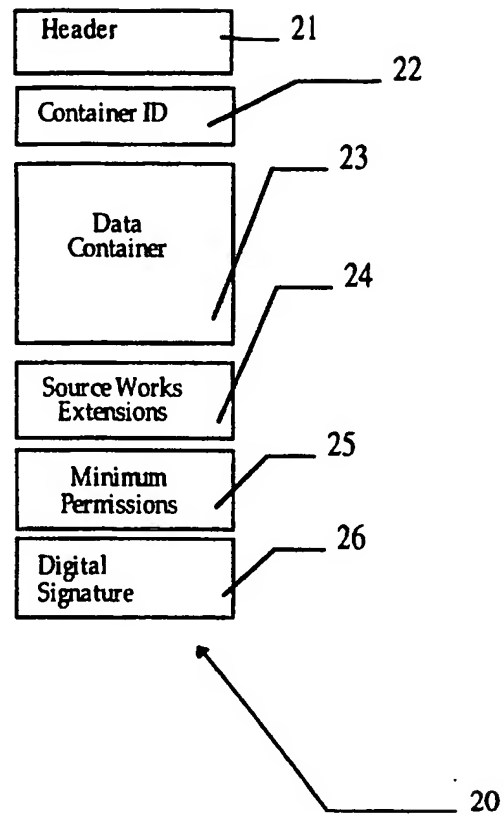
Figure 1A

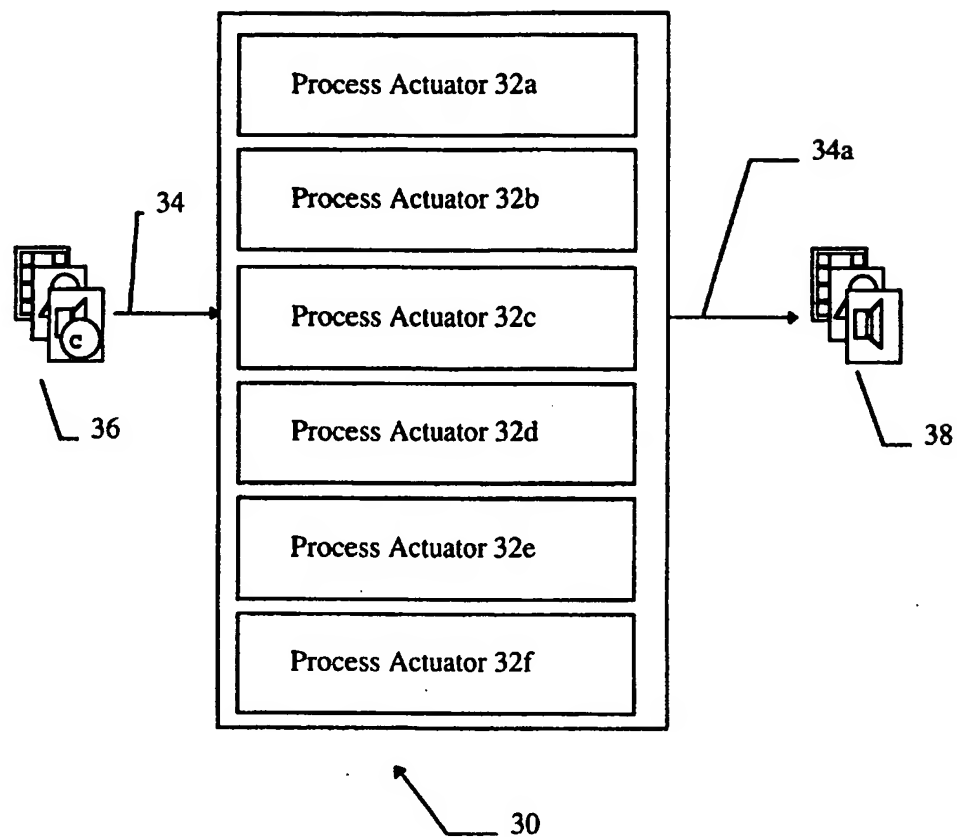
Figure 2

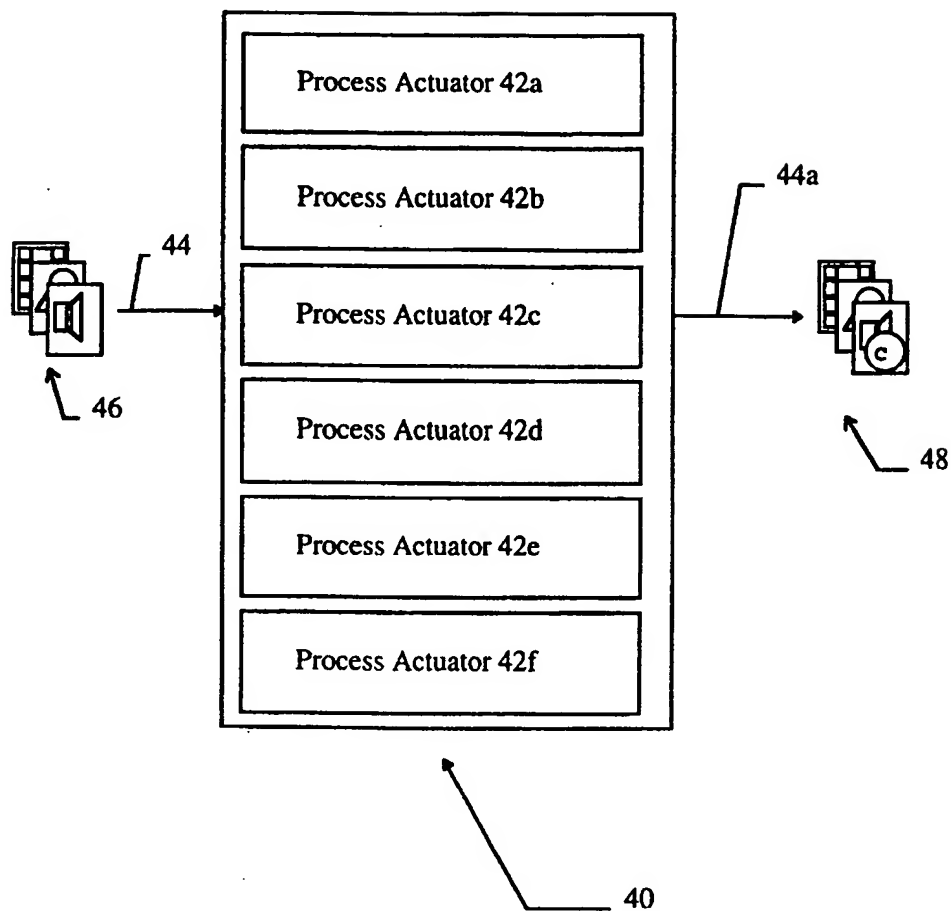
Figure 3

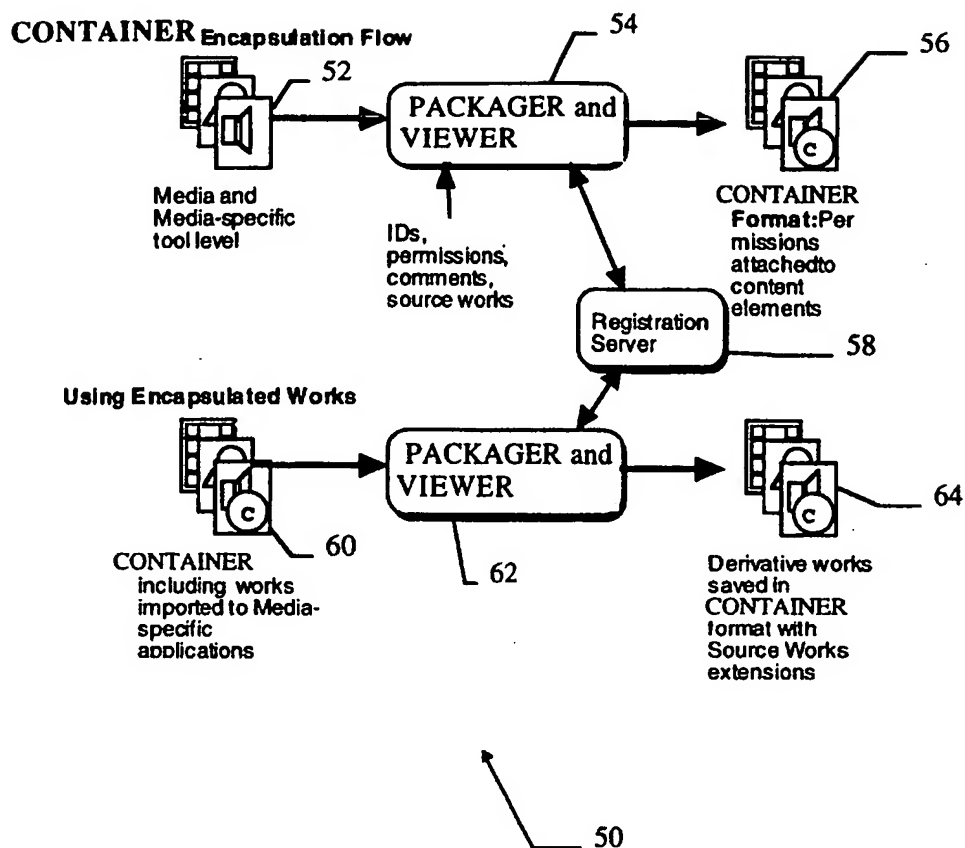
Figure 4

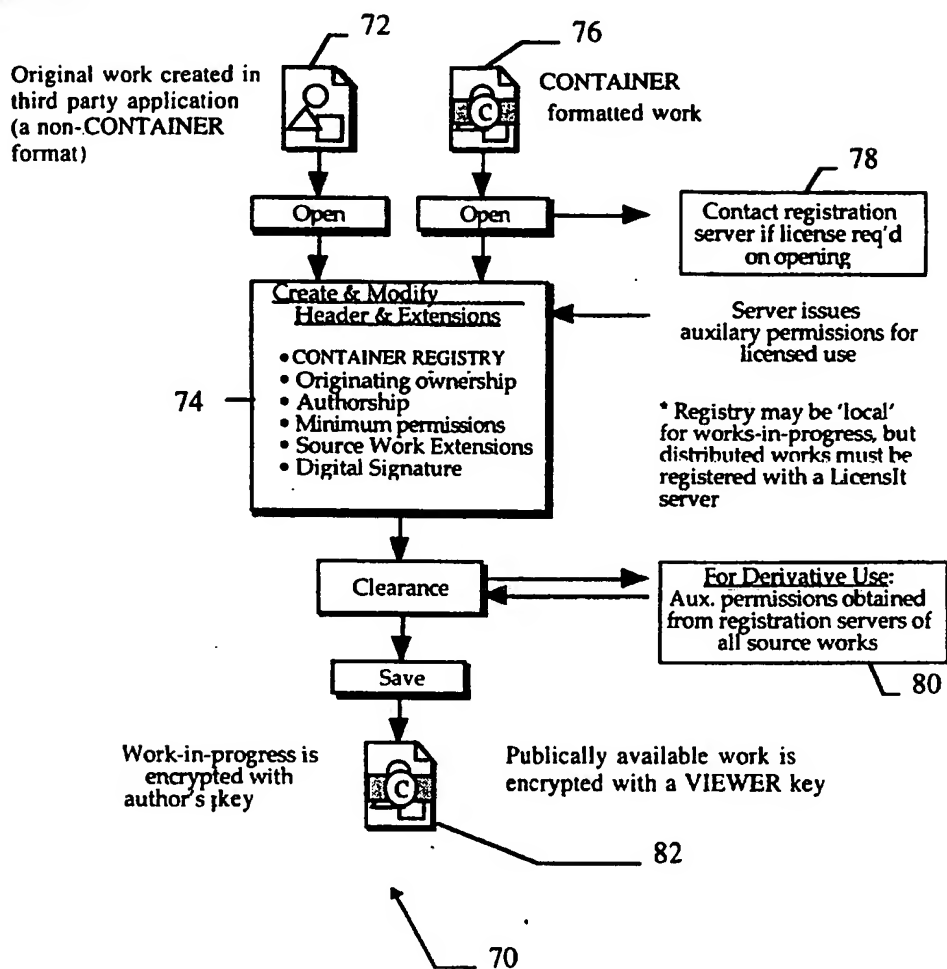
Figure 5

Figure 5a

Licensit DocInfo Editor

CONTAINER Licensit Rev: 0.1

CONTAINER ID:
Server: 129.170.56.64 Doc: 1

CONTAINER Comments:
Vernont.pict © 1995 Norwich Mountain Technologies.
All Rights Reserved.
If you don't believe me, notice

Data Format: PICT (50KBytes)

Minimum Permissions:

<input checked="" type="checkbox"/> Read Only	<input checked="" type="checkbox"/> Allow Collab
<input type="checkbox"/> Local Only	<input type="checkbox"/> Source Works
<input checked="" type="checkbox"/> Lic. on Save	<input checked="" type="checkbox"/> Register on Save
<input type="checkbox"/> Lic. on View	<input type="checkbox"/> Original Format

Edit Source Works

Cancel Okoy

Figure 5b

Licensit Doc Info

CONTAINER Licensit Rev: 0.1

CONTAINER ID:
Server: 129.170.56.64 Doc: 1

CONTAINER Comments:
Vernont.pict © 1995 Norwich Mountain Technologies.
All Rights Reserved.
If you don't believe me, notice

Data Format: PICT (50KBytes)

Minimum Permissions:

<input checked="" type="radio"/> Read Only	<input checked="" type="radio"/> Allow Collab
<input type="radio"/> Local Only	<input type="radio"/> Source Works
<input checked="" type="radio"/> Lic. on Save	<input checked="" type="radio"/> Register on Save
<input type="radio"/> Lic. on View	<input type="radio"/> Original Format

Auxiliary Perms Source Works

Figure 6

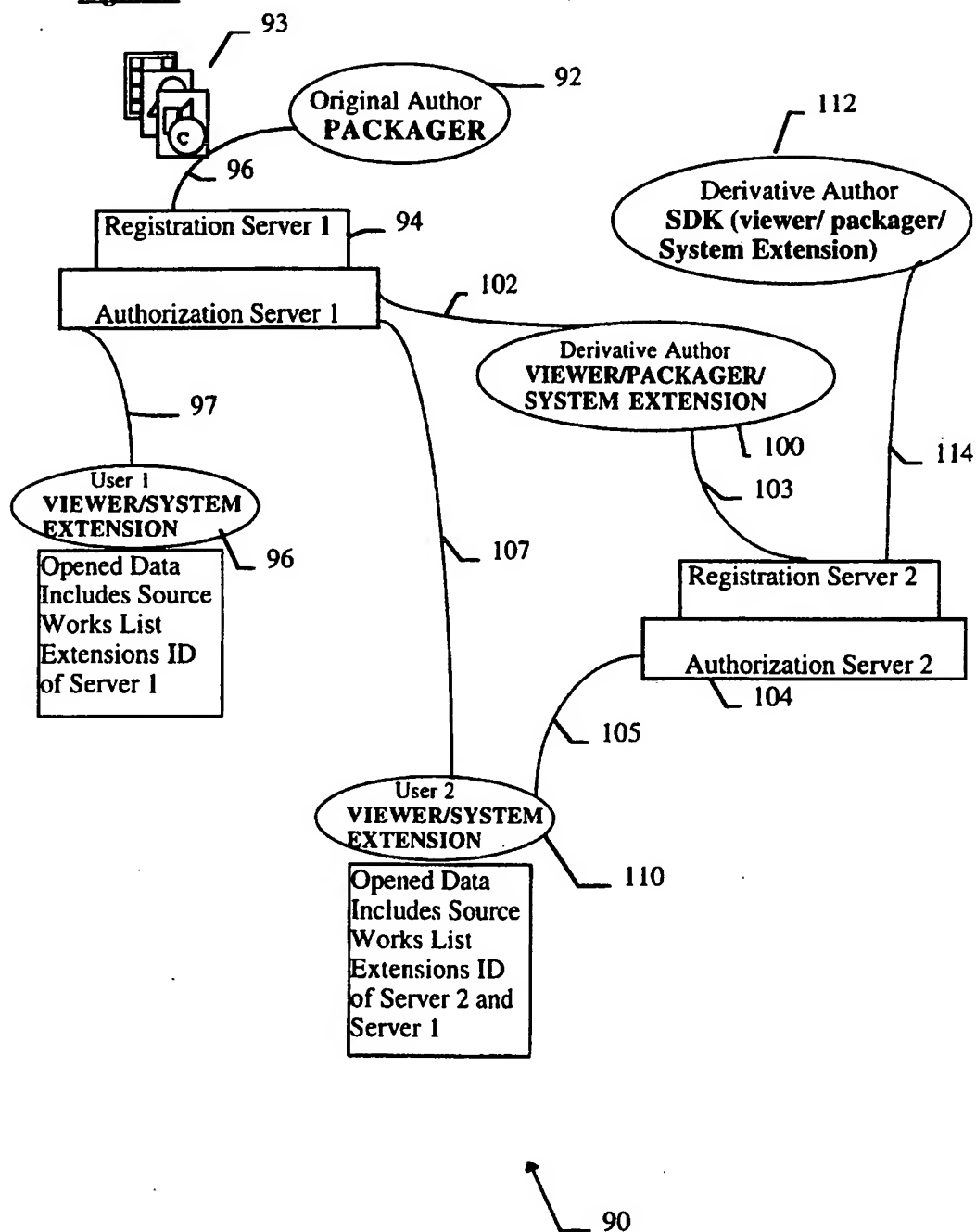


Figure 7

A dialog box titled "CONTAINER Info" with a standard Windows-style title bar. The dialog contains several input fields and buttons. The fields are arranged in two columns: "Title:" and "License Rev:" on the top row, "Author:" and "Media Type:" on the second row, "Registry:" and "Creator App:" on the third row, and a "Comments:" label followed by a large text area on the fourth row. Below the text area is a "Current Permissions:" label followed by another large text area. At the bottom, there are three buttons: "Display Sources", "Registry Info" (which is highlighted with a double border), and "License!!".

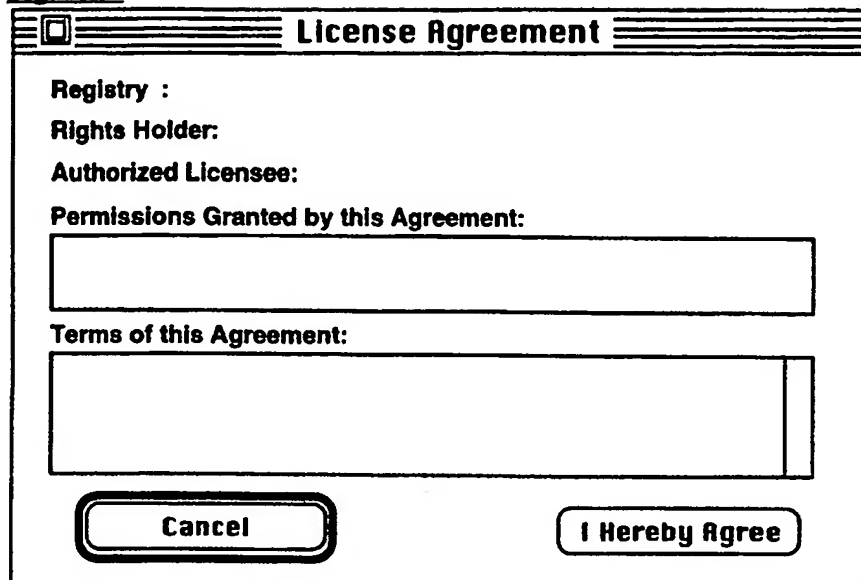
Figure 7a

A dialog box titled "License Request" with a standard Windows-style title bar. The dialog contains a "Registry:" label followed by a "Permissions Requested:" label and a large text area for input. At the bottom, there are three buttons: "Edit Request", "Cancel" (highlighted with a double border), and "Submit".

Figure 7b

A dialog box titled "Permissions Request Editor" with a standard Windows-style title bar. The dialog contains a "Permissions Requested:" label followed by two columns of checkboxes. The left column has five checkboxes labeled "Opening/Viewing", "Modify", "Drag & Drop", "Printing", and "Format Changes". The right column has five checkboxes, with the top one labeled "Save". At the bottom, there are two buttons: "Cancel" and "Okay" (highlighted with a double border).

Figure 7c



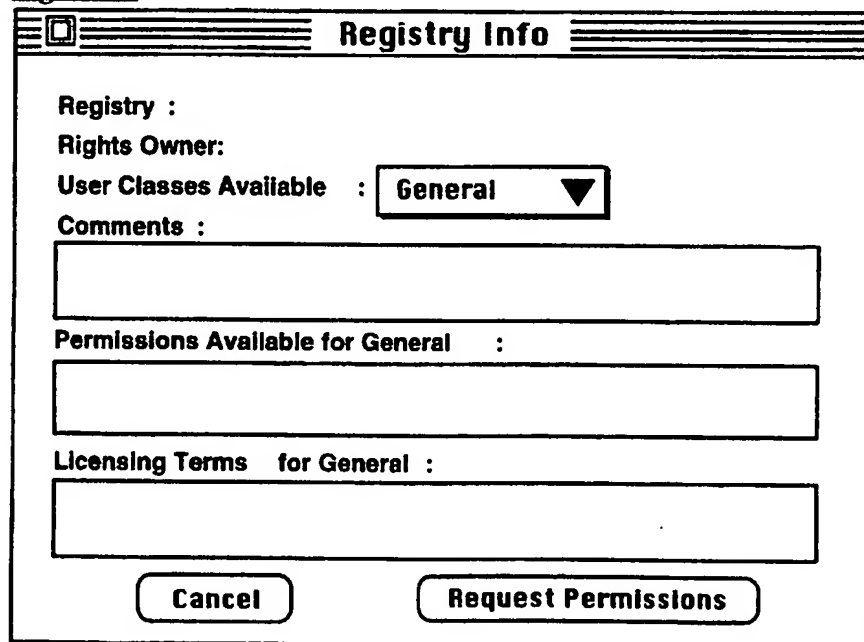
License Agreement

Registry :
Rights Holder:
Authorized Licensee:
Permissions Granted by this Agreement:

Terms of this Agreement:

Cancel **I Hereby Agree**

Figure 7d



Registry Info

Registry :
Rights Owner:
User Classes Available : **General** ▼
Comments :

Permissions Available for General :

Licensing Terms for General :

Cancel **Request Permissions**

Figure 7e

Source Works Display			
Container	ID :	Title :	Registry :
sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc
sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc
sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc
sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc
sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc

Registry Info

Request Permissions

Figure 7f

Source Works Manager				
Container	ID :	Title :	Registry :	Clearance :
sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc	Okay
sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc	Okay
sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc	Failed
sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc	Okay
sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc	sdcsdcsfzczdc	Okay

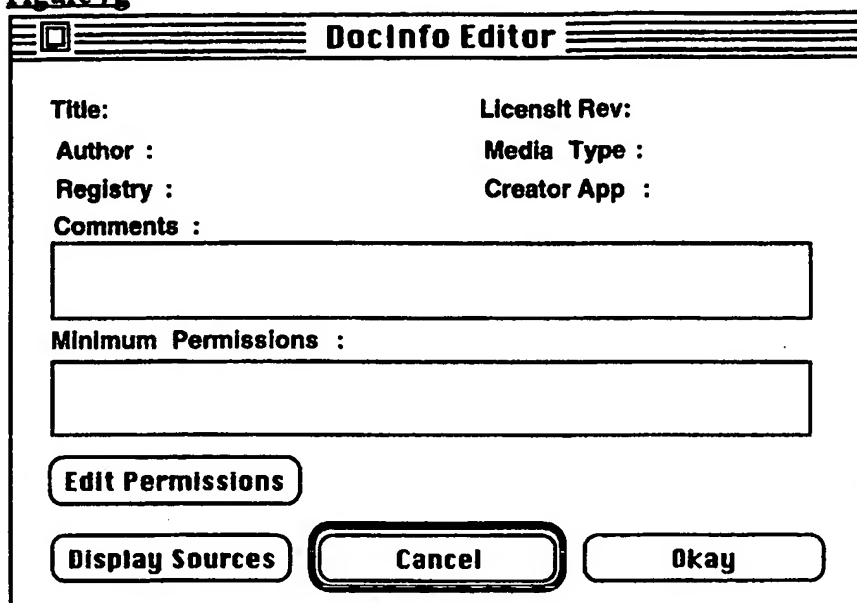
Registry Info

Check Clearances

Permissions Info

Request Permissions

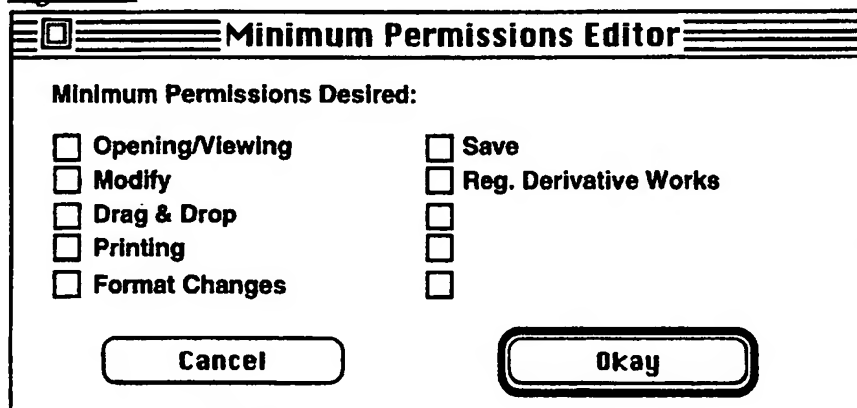
Figure 7g



The **DocInfo Editor** dialog box contains the following fields and controls:

- Title:** [Text Field]
- Author :** [Text Field]
- Registry :** [Text Field]
- Comments :** [Text Field]
- License Rev:** [Text Field]
- Media Type :** [Text Field]
- Creator App :** [Text Field]
- Minimum Permissions :** [Text Field]
- Edit Permissions** button
- Display Sources** button
- Cancel** button
- Okay** button

Figure 7h



The **Minimum Permissions Editor** dialog box contains the following controls:

Minimum Permissions Desired:

<input type="checkbox"/> Opening/Viewing	<input type="checkbox"/> Save
<input type="checkbox"/> Modify	<input type="checkbox"/> Reg. Derivative Works
<input type="checkbox"/> Drag & Drop	<input type="checkbox"/>
<input type="checkbox"/> Printing	<input type="checkbox"/>
<input type="checkbox"/> Format Changes	<input type="checkbox"/>

Cancel button **Okay** button

Figure 8

Third Party Application - Actions	VIEWER and/or PACKAGER Actions	Authorization Server Actions	Registration Server Actions
CONTAINER Opened	VIEWER views CONTAINER attributes, including minimum and auxiliary permissions, if any		
	Authorization server contacted if required	Compute requested permissions and user class with rule base	
		Grant appropriate auxiliary permissions and issue encrypted certificate	
Viewer or editor opened for packaged data type	If editing, initialize local list of active source works		
Attempt unauthorized action			
Prepare request for required permissions	Contact authorization server for auxiliary permissions	Compare requested permissions and user class with rule base	
		Grant appropriate auxiliary permissions and issue encrypted certificate	
Perform desired action			
Import CONTAINER	Contact authorization server on opening, if required		
	Add new work to Source Works list		
Attempt file save	Examine clearances (minimum and auxiliary permissions) of source works		
	Initiate authorization requests for unclosed works	Grant appropriate auxiliary permissions and issue encrypted certificate	
Move data to Packager	Assemble based upon data to be saved		
	Select server and generate registration request		Grant registration request (used for final signature)
	Complete CONTAINER packaging		

Figure 9

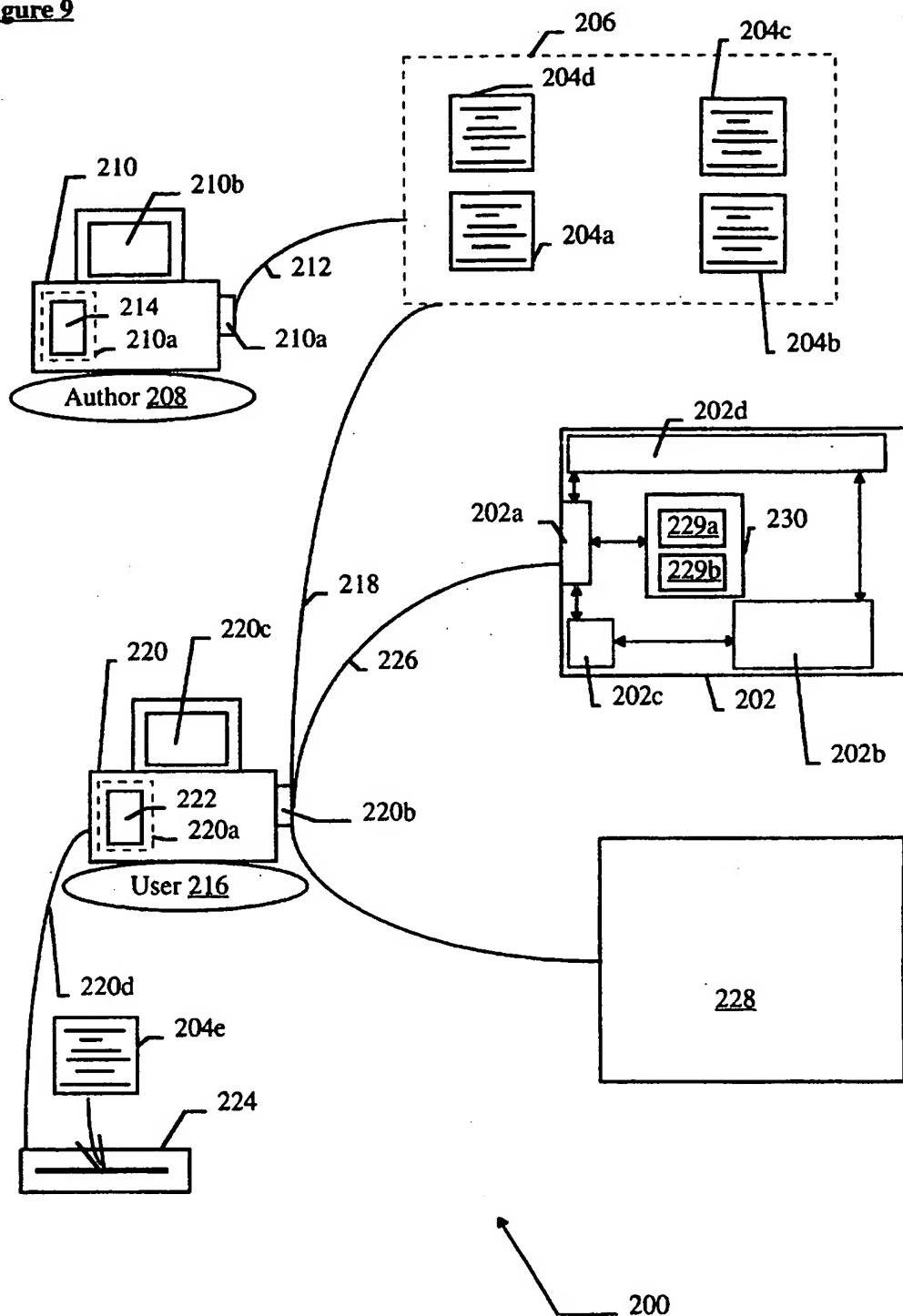


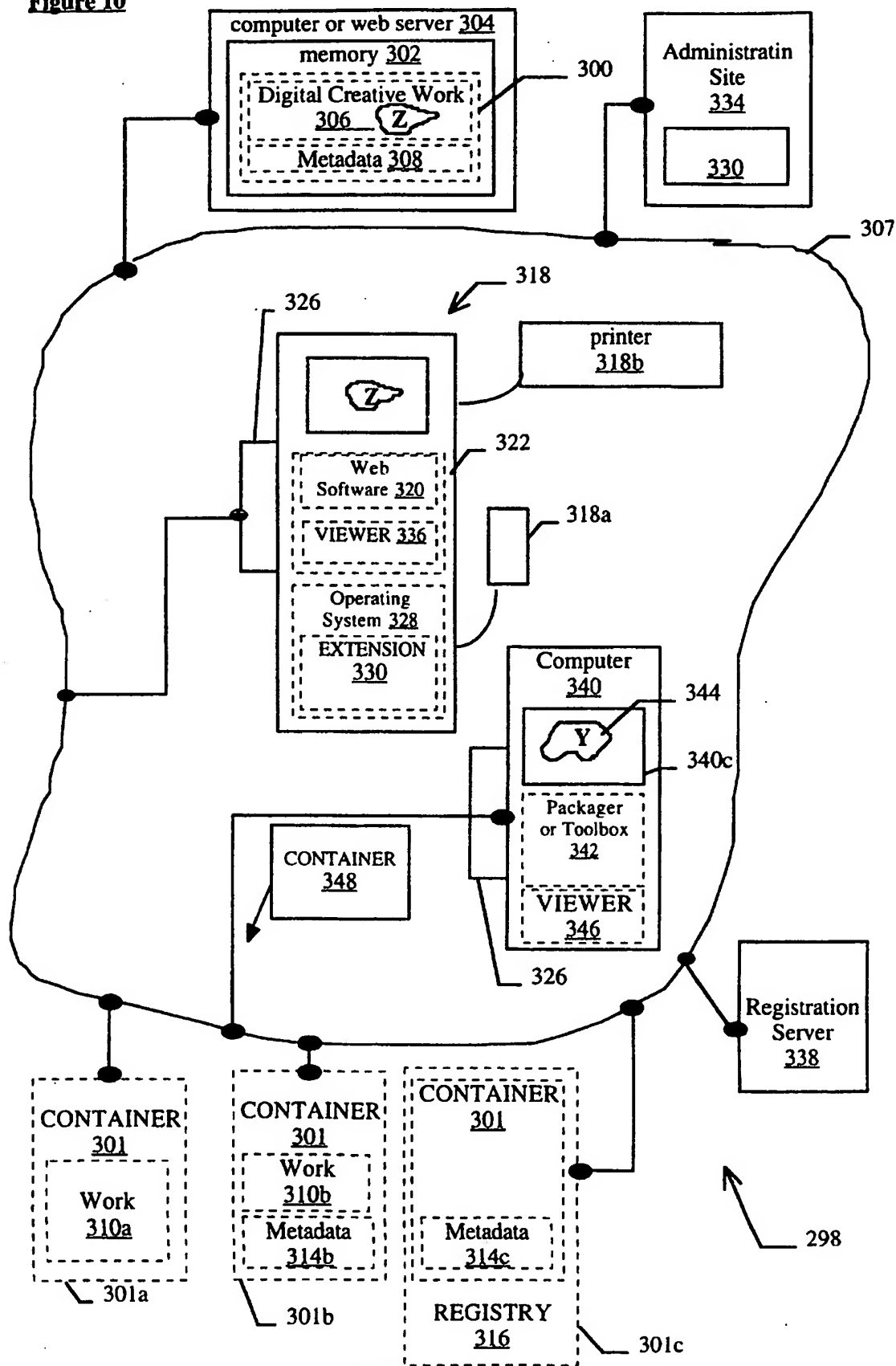
Figure 10

FIG. 11

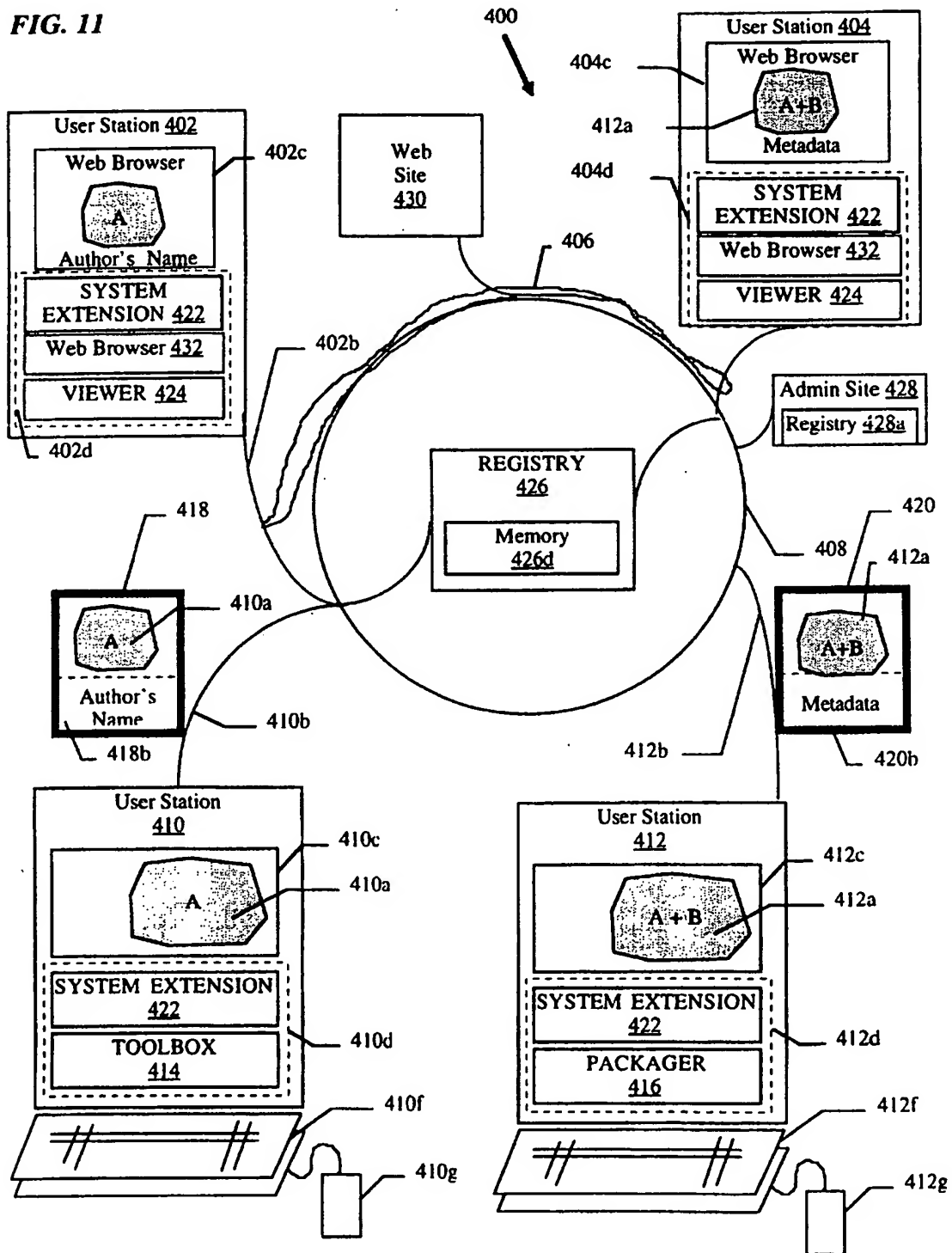


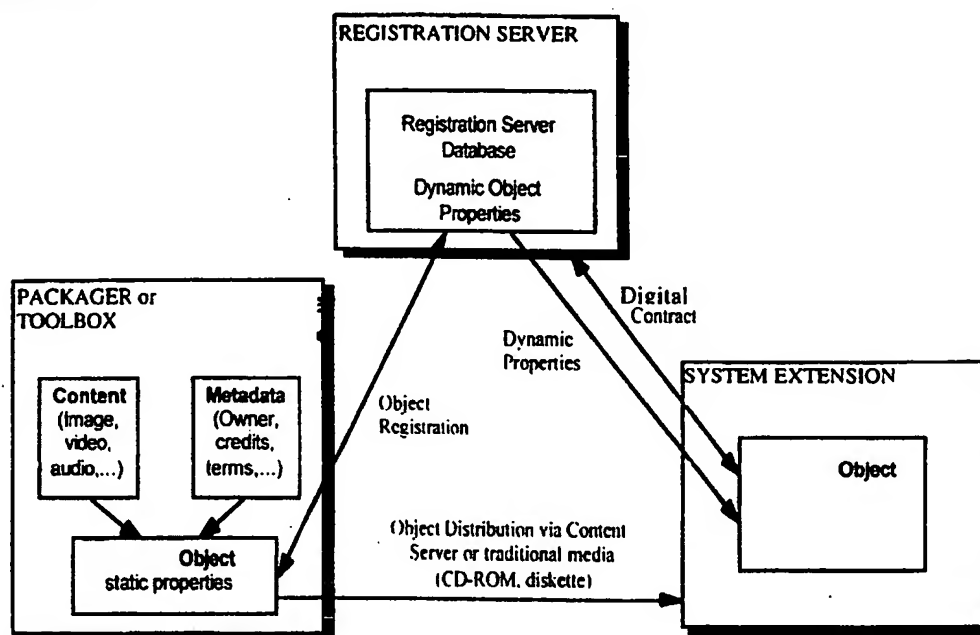
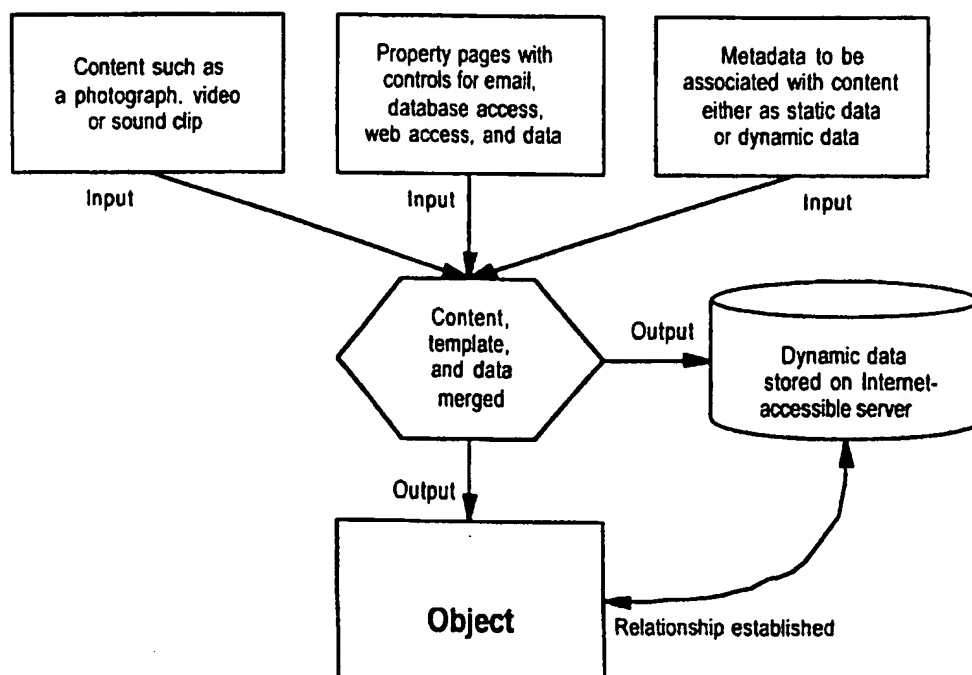
Figure 12**Figure 13**

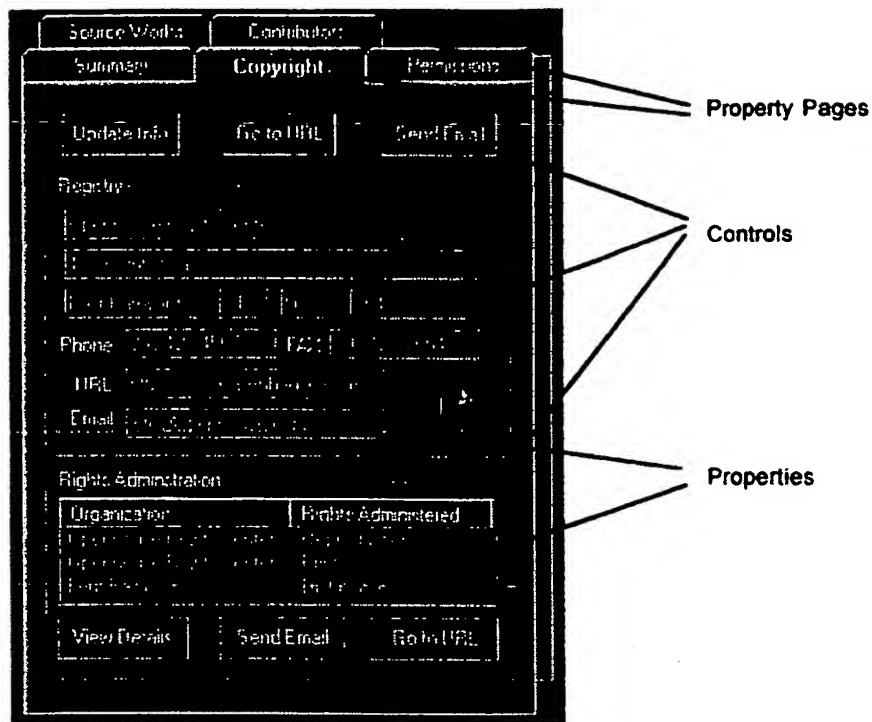
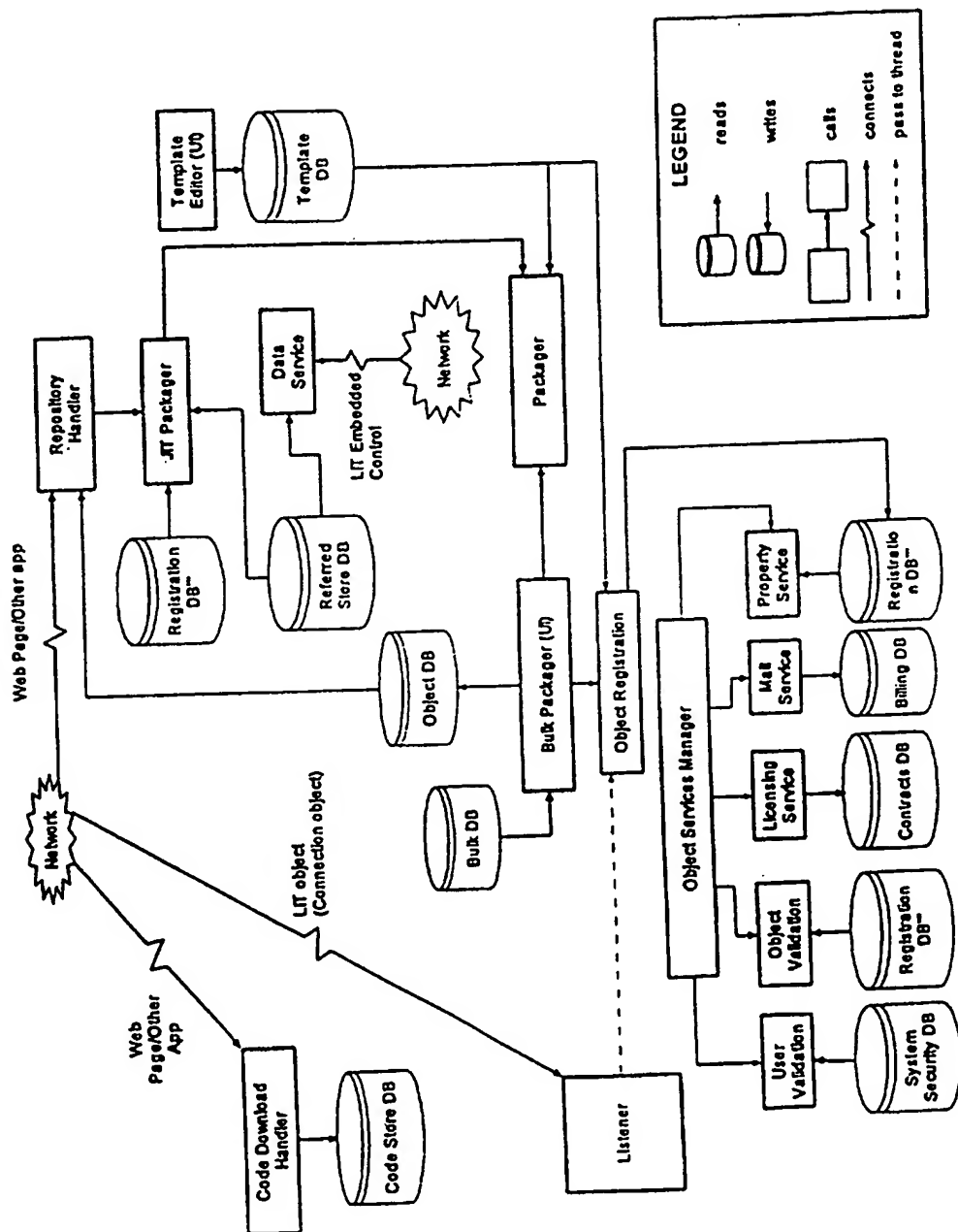
Figure 14**Figure 15**

Figure 16



INTERNATIONAL SEARCH REPORT

International Application No
PC/US 96/16348

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00 G06F17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO,A,94 27228 (APPLE COMPUTER) 24 November 1994 see page 6, line 12 - page 9, line 9 see page 29, line 6 - page 33, line 3 see page 47, line 5 - page 52, line 12 ---	1-146
Y	IEEE NETWORK, MAY-JUNE 1995, USA, vol. 9, no. 3, ISSN 0890-8044, pages 12-20, XP000505280 CHOUDHURY A K ET AL: "Copyright protection for electronic publishing over computer networks" see the whole document ---	1-146
A	US,A,5 023 907 (JOHNSON HERRICK J ET AL) 11 June 1991 see column 1, line 10 - column 2, line 36 ---	1-146
-/--		

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- *&* document member of the same patent family

Date of the actual completion of the international search

3 February 1997

Date of mailing of the international search report

18.02.97

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Fournier, C

INTERNATIONAL SEARCH REPORT

International Application No
PC1/US 96/16348

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>IBM TECHNICAL DISCLOSURE BULLETIN, vol. 37, no. 3, 1 March 1994, pages 413-417, XP000441522 "MULTIMEDIA MIXED OBJECT ENVELOPES SUPORTING A GRADUATED FEE SCHEME VIA ENCRYPTION" see the whole document -----</p>	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 96/16348

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO-A-9427228	24-11-94	AU-A- 6826694 EP-A- 0698242	12-12-94 28-02-96
US-A-5023907	11-06-91	NONE	

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.